(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11284666 A**
(43) Date of publication of application: **15.10.1999**

(51) Int. Cl **H04L 12/66**
H04L 12/46, H04L 12/28, H04L 12/56, H04M 3/00, H04M 11/00, H04Q 7/34

(21) Application number: **10306446**
(22) Date of filing: **14.10.1998**
(30) Priority: **14.10.1997 US 97 61915**
24.08.1998 US 98 138536

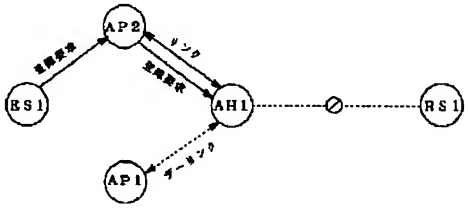
(71) Applicant: **LUCENT TECHNOL INC**
(72) Inventor: **CHUAH MOOI CHOO**
RAI GIRISH

(54) MOBILE MANAGEMENT SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a variety of remote radio accesses to an end user by dividing mobility management to categories of four connection handover consisting local, micro, macro and global to minimize update of hand-off accordingly.

SOLUTION: First a data frame is communicated between a 1st mobile end system ES1 and a 1st access hub AH1, then when the 1st mobile end system ES1 is moved and makes registration again through a 2nd access point AP2, a registration request is sent to the 1st access hub from the 1st mobile end system ES1 through the 2nd access point. The 1st mobile end system ES1 is registered again to the 1st access hub without notice of a 1st registration server. Then the 2nd access point is linked with the 1st access hub and the link between the 1st access point and the 1st access hub is interrupted.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－284666

(43)公開日　平成11年(1999)10月15日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　11/20	Ｂ
12/46		Ｈ０４Ｍ　3/00	Ｄ
12/28		11/00	３０３
12/56		Ｈ０４Ｌ　11/00	３１０Ｃ
Ｈ０４Ｍ　3/00			３１０Ｂ

審査請求　未請求　請求項の数28　ＯＬ　外国語出願　（全218頁）　最終頁に続く

(21)出願番号　特願平10－306446

(22)出願日　平成10年(1998)10月14日

(31)優先権主張番号　６０／０６１９１５

(32)優先日　1997年10月14日

(33)優先権主張国　米国（ＵＳ）

(31)優先権主張番号　０９／１３８５３６

(32)優先日　1998年８月24日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　596092698
ルーセント　テクノロジーズ　インコーポレーテッド
アメリカ合衆国．07974－0636　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　600

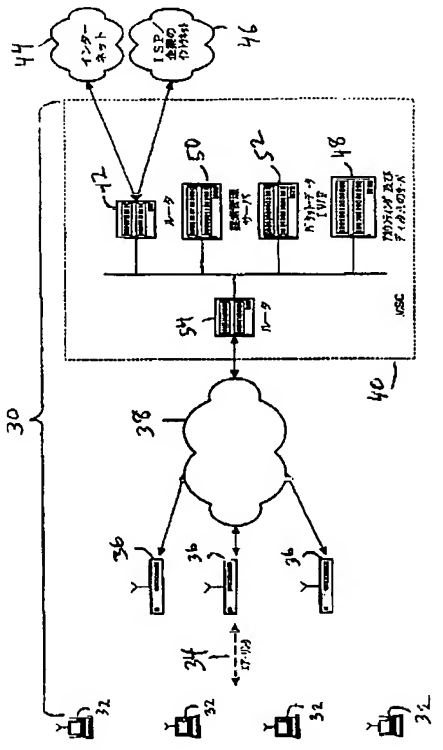
(72)発明者　ムーイ　チョー　チュアー
アメリカ合衆国　07724　ニュージャーシィ，イートンタウン，イートンクレスト　ドライヴ　184ビー

(74)代理人　弁理士　岡部　正夫　（外11名）

最終頁に続く

(54)【発明の名称】　移動管理システム

(57)【要約】　（修正有）
【課題】パケット交換データネットワーク内でのモバイルエンドシステムを管理する。
【解決手段】最初はデータフレームをモバイルエンドシステム３２と第一アクセスポイント３４を通じてアクセスハブとの間で通信し、アクセスハブを含む第一モジュール３６が、登録リクエストがモバイルエンドから第二アクセスポイント３８を通じて受信されたとき、モバイルエンドを第一アクセスハブに、第一登録サーバに通知することなく再登録し、第一アクセスハブがさらに第二モジュールを含み、第二モジュールが、モバイルエンドが再登録されたとき、第二アクセスポイントを第一アクセスハブにリンクし、第一アクセスハブがさらに第三モジュール４０を含み、この第三モジュールが、第二アクセスポイントが第一アクセスハブにリンクされたとき、第一アクセスポイントと第一アクセスハブ間のリンクを切断する。



【特許請求の範囲】

【請求項１】　通信システムであって、このシステムが：第一の登録サーバ、第一と第二のアクセスポイント、および第一のアクセスハブを含むネットワークから構成され、このネットワークが最初はデータフレームを第一のモバイルエンドシステムと第一のアクセスポイントを通じて第一のアクセスハブとの間で通信しており；前記第一のアクセスハブが第一のモジュールを含み、この第一のモジュールが、登録リクエストが前記第一のモバイルエンドシステムから前記第二のアクセスポイントを通じて受信されたとき、前記第一のモバイルエンドシステムを前記第一のアクセスハブに、前記第一の登録サーバに通知することなく、再登録し；前記第一のアクセスハブがさらに第二のモジュールを含み、この第二のモジュールが、前記モバイルエンドシステムが前記第二のアクセスポイントを通じて再登録されたとき、前記第二のアクセスポイントを前記第一アクセスハブにリンクし；前記第一のアクセスハブがさらに第三のモジュールを含み、この第三のモジュールが、前記第二のアクセスポイントが前記第一のアクセスハブにリンクされたとき、前記第一のアクセスポイントと前記第一のアクセスハブの間のリンクを切断することを特徴とするシステム。

【請求項２】　前記ネットワークがフォーリンネットワークと見なされ、このフォーリンネットワークがさらに第二と第三のアクセスハブおよび第一のインターワーキング機能を含み、このフォーリンネットワークが最初はデータフレームを第二のモバイルエンドシステムと第二のアクセスハブを通じて前記第一のインターワーキング機能との間で通信しており；ホームネットワークがホーム登録サーバを含み；前記第一の登録サーバが第一のモジュールを含み、この第一のモジュールが、登録リクエストが第二のモバイルエンドシステムから第三のアクセスポイントおよび第三のアクセスハブを通じて受信されたとき、前記第二のモバイルエンドシステムを前記第一の登録サーバに、前記ホーム登録サーバに通知することなく、再登録し；前記第一の登録サーバがさらに第二のモジュールを含み、この第二のモジュールが、前記第二のモバイルエンドシステムが前記第三のアクセスハブを通じて再登録されたとき、前記第三のアクセスハブに対して前記第一のインターワーキング機能とリンクすることを指令し；前記第一の登録サーバがさらに第三のモジュールを含み、この第三のモジュールが、前記第三のアクセスハブと前記第一のインターワーキング機能とがリンクされた後に、前記第二のアクセスハブに対して前記第一のインターワーキング機能とのリンクを切断することを指令することを特徴とする請求項１のシステム。

【請求項３】　前記フォーリンネットワークがさらに第四のアクセスハブおよび第二と第三のインターワーキング機能を含み；前記ホームネットワークがさらに第四のインターワーキング機能を含み、前記フォーリンネットワークは最初はデータフレームを第三のモバイルエンドシステムと前記第二のインターワーキング機能を通じて前記第四のインターワーキング機能との間で通信しており、ホームネットワークは最初はデータフレームを前記第四のインターワーキング機能と第一の通信サーバとの間で通信しており；前記ホーム登録サーバが第一のモジュールを含み、この第一のモジュールが、登録リクエストが前記第三のモバイルエンドシステムから第四のアクセスポイント、第四のアクセスハブおよび第一の登録サーバを通じて受信されたとき、前記第三のモバイルエンドシステムを前記ホーム登録サーバに、前記第四のインターワーキング機能と前記第一の通信サーバとの間のリンクを切断することなく、再登録し、前記第一のモジュールが、前記登録リクエスト内の前記第二のインターワーキング機能から第三のインターワーキング機能への変更を示す指標を認識し；前記ホーム登録サーバがさらに第二のモジュールを含み、この第二のモジュールが、前記第三のモバイルエンドシステムが前記第四のアクセスハブを通じて再登録されたとき、前記第四のインターワーキング機能に対して前記第三のインターワーキング機能とリンクすることを指令し；前記ホーム登録サーバがさらに第三のモジュールを含み、この第三のモジュールが、前記第三のインターワーキング機能が前記第四のインターワーキング機能とリンクされた後に、前記第四のインターワーキング機能に対して前記第二のインターワーキング機能との間のリンクを切断することを指令することを特徴とする請求項２のシステム。

【請求項４】　前記フォーリンネットワークが第一のフォーリンネットワークと見なされ、この第一のフォーリンネットワークがさらに第五のインターワーキング機能を含み；第二のフォーリンネットワークが第二の登録サーバ、第五のアクセスハブおよび第六のインターワーキング機能を含み；前記ホームネットワークがさらに第七のインターワーキング機能を含み、第一のフォーリンネットワークは最初はデータフレームを第四のモバイルエンドシステムと第五のインターワーキング機能を通じて第七のインターワーキング機能との間で通信しており、ホームネットワークは最初はデータフレームを第七のインターワーキング機能と第二の通信サーバとの間で通信しており；前記ホームネットワークがさらに第四のモジュールを含み、この第四のモジュールが、登録リクエストが前記第四のモバイルエンドシステムから第五のアクセスポイント、第五のアクセスハブおよび第二の登録サーバを通じてホーム登録サーバに受信されたとき、前記第四のモバイルエンドシステムを前記ホーム登録サーバに、前記第七のインターワーキング機能を前記第二の通信サーバから切断することなく、再登録し；前記ホーム登録サーバがさらに第五のモジュールを含み、この第五のモジュールが、前記第四のモバイルエンドシステムが

前記第五のアクセスハブを通じて再登録されたとき、前記第七のインターワーキング機能に対して前記第六のインターワーキングとリクンすることを指令し；前記ホーム登録サーバがさらに第六のモジュールを含み、この第六のモジュールが、前記第六のインターワーキング機能が前記第七のインターワーキング機能とリンクされた後に、前記第七のインターワーキング機能に対して前記第五のインターワーキング機能との間のリンクを切断することを指令することを特徴とする請求項３のシステム。

【請求項５】　前記フォーリンネットワークが第一のフォーリンネットワークと見なされ、この第一のフォーリンネットワークがさらに第五のインターワーキング機能を含み；第二のフォーリンネットワークが第二の登録サーバ、第五のアクセスハブおよび第六のインターワーキング機能を含み；前記ホームネットワークがさらに第七と第八のインターワーキング機能を含み、前記第一のフォーリンネットワークは最初データフレームを第四のモバイルエンドシステムと前記第五のインターワーキング機能を通じて前記第七のインターワーキング機能との間で通信しており、前記ホームネットワークは最初データフレームを前記第七のインターワーキング機能と第二の通信サーバとの間で通信しており；前記ホームサーバがさらに第四のモジュールを含み、この第四のモジュールが、登録リクエストが前記第四のモバイルエンドシステムから第五のアクセスポイント、前記第五のアクセスハブおよび前記第二の登録サーバを通じて前記ホーム登録サーバに受信されたとき、前記第四のモバイルエンドシステムを前記ホーム登録サーバと再登録し；前記ホーム登録サーバがさらに第五のモジュールを含み、この第五のモジュールが、前記第四のモバイルエンドシステムが前記第五のアクセスハブを通じて再登録されたとき、前記第八のインターワーキング機能に対して前記第六のインターワーキング機能とリンクすることを指令し；前記ホーム登録サーバがさらに第六のモジュールを含み、この第六のモジュールが、前記第八のインターワーキング機能に対して前記第二の通信リンクとリンクすることを指令し；前記ホーム登録サーバがさらに第七のモジュールを含み、この第七のモジュールが、前記第七のインターワーキング機能に対して前記第二の通信サーバとの間のリンクを切断することを指令し；前記ホーム登録サーバがさらに第八のモジュールを含み、この第八のモジュールが、前記第八のインターワーキング機能が前記第六のインターワーキング機能とリンクされた後に、前記第七のインターワーキング機能に対して前記第五のインターワーキング機能との間のリンクを切断することを指令することを特徴とする請求項３のシステム。

【請求項６】　通信システムであって：フォーリンネットワークが第一の登録サーバ、第一と第二のアクセスハブおよび第一のインターワーキング機能を含み、このフォーリンネットワークが最初はデータフレームを第一のモバイルエンドシステムと第一のアクセスハブを通じて前記第一のインターワーキング機能との間で通信しており；ホームネットワークがホーム登録サーバを含み；前記第一の登録サーバが第一のモジュールを含み、この第一のモジュールが、登録リクエストが前記第一のモバイルエンドシステムから第一のアクセスポイントおよび第二のアクセスハブを通じて前記第一の登録サーバに受信されたとき、前記第一のモバイルエンドシステムを前記第一の登録サーバに、前記ホーム登録サーバに通知することなく、再登録し；前記第一の登録サーバがさらに第二のモジュールを含み、この第二のモジュールが、前記第一のモバイルエンドシステムが前記第二のアクセスハブを通じて再登録されたとき、前記第二のアクセスハブに対して前記第一のインターワーキング機能とリンクすることを指令し；前記第一の登録サーバがさらに第三のモジュールを含み、この第三のモジュールが、前記第二のアクセスハブが前記第一のインターワーキング機能とリンクされた後に、前記第一のアクセスハブに対して前記第一のインターワーキング機能との間のリンクを切断することを指令することを特徴とするシステム。

【請求項７】　前記フォーリンネットワークがさらに第三のアクセスハブと、第二および第三のインターワーキング機能を含み；前記ホームネットワークがさらに第四のインターワーキング機能を含み、前記フォーリンネットワークが最初はデータフレームを第二のモバイルエンドシステムと前記第二のインターワーキング機能を通じて前記第四のインターワーキング機能との間で通信しており、前記ホームネットワークは最初データフレームを前記第四のインターワーキング機能と第一の通信サーバとの間で通信しており；前記ホーム登録サーバが第一のモジュールを含み、この第一のモジュールが、登録リクエストが前記第二のモバイルエンドシステムから第二のアクセスポイント、前記第三のアクセスハブおよび前記第一の登録サーバを通じて前記ホーム登録サーバに受信されたとき、前記第二のモバイルエンドシステムを、前記ホーム登録サーバに、前記第四のインターワーキング機能と前記第一の通信サーバとの間のリンクを切断することなく、再登録し、前記第一のモジュールは前記登録リクエスト内の前記第二のインターワーキング機能から前記第三のインターワーキング機能への変更を示す指標に認識し；前記ホーム登録サーバがさらに第二のモジュールを含み、この第二のモジュールが、前記第二のモバイルエンドシステムが前記第三のアクセスハブを通じて再登録されたとき、前記第三のインターワーキング機能に対して前記第四のインターワーキング機能とリンクすることを指令し；前記ホーム登録サーバがさらに第三のモジュールを含み、この第三のモジュールが、前記第三のインターワーキング機能が前記第四のインターワーキング機能とリンクされた後に、前記第二のインターワーキング機能に対して前記第四のインターワーキング機能

とのリンクを切断することを指令することを特徴とする請求項６のシステム。

【請求項８】　前記フォーリンネットワークが第一のフォーリンネットワークと見なされ、この第一のフォーリンネットワークがさらに第五のインターワーキング機能を含み；第二のフォーリンネットワークが、第二の登録サーバ、第四のアクセスハブおよび第六のインターワーキング機能を含み；前記ホームネットワークがさらに第七のインターワーキング機能を含み、前記第一のフォーリンネットワークが最初はデータフレームを第三のモバイルエンドシステムと前記第五のインターワーキング機能を通じて前記第七のインターワーキング機能との間で通信しており、前記ホームネットワークは最初はデータフレームを前記第七のインターワーキング機能と第二の通信サーバとの間で通信しており；前記ホーム登録サーバが第四のモジュールを含み、この第四のモジュールが、登録リクエストが前記第三のエンドシステムから第三のアクセスポイント、前記第四のアクセスハブおよび前記第二の登録サーバを通じて前記ホーム登録サーバに受信されたとき、前記第三のモバイルエンドシステムを前記ホーム登録サーバに、前記第七のインターワーキング機能と前記第二の通信サーバとの間のリンクを切断することなく、再登録し；前記ホーム登録サーバがさらに第五のモジュールを含み、この第五のモジュールが、前記第三のモバイルエンドシステムが前記第四のアクセスハブを通じて再登録されたとき、前記第六のインターワーキング機能に対して前記第七のインターワーキング機能とリンクすることを指令し；前記ホーム登録サーバがさらに第六のモジュールを含み、この第六のモジュールが、前記第六のインターワーキング機能が前記第七のインターワーキング機能とリンクされた後に、前記第五のインターワーキング機能に対して前記第七のインターワーキング機能との間のリンクを切断することを指令することを特徴とする請求項７のシステム。

【請求項９】　前記フォーリンネットワークが第一のフォーリンネットワークと見なされ、前記第一のフォーリンネットワークがさらに第五のインターワーキング機能を含み；第二のフォーリンネットワークが第二の登録サーバ、第四のアクセスハブおよび第六のインターワーキング機能を含み；前記ホームネットワークがさらに第七および第八のインターワーキング機能を含み、前記第一のフォーリンネットワークは最初はデータフレームを第三のモバイルエンドシステムと前記第五のインターワーキング機能を通じて前記第七のインターワーキング機能との間で通信しており、前記ホームネットワークは最初はデータフレームを前記第七のインターワーキング機能と第二の通信サーバとの間で通信しており；前記ホーム登録サーバがさらに第四のモジュールを含み、この第四のモジュールが、登録リクエストが前記第三のモバイルエンドシステムから第三のアクセスポイント、前記第四のアクセスハブ、および前記第二の登録サーバを通じて前記ホーム登録サーバに受信されたとき、前記第三のモバイルエンドシステムを前記ホーム登録サーバに再登録し；前記ホーム登録サーバがさらに第五のモジュールを含み、この第五のモジュールが、前記第三のモバイルエンドシステムが前記第四のアクセスハブを通じて再登録されたとき、前記第八のインターワーキング機能に対して前記第六のインターワーキング機能とリンクすることを指令し；前記ホーム登録サーバがさらに第六のモジュールを含み、この第六のモジュールが前記第八のインターワーキング機能に対して前記第二の通信サーバとリンクすることを指令し；前記ホーム登録サーバがさらに第七のモジュールを含み、この第七のモジュールが、前記第七のインターワーキング機能に対して前記第二の通信サーバとの間のリンクを切断することを指令し；前記ホーム登録サーバがさらに第八のモジュールを含み、この第八のモジュールが、前記第八のインターワーキング機能が前記第六のインターワーキング機能とリンクされた後に、前記第七のインターワーキング機能に対して前記第五のインターワーキング機能との間のリンクを切断することを指令することを特徴とする請求項７のシステム。

【請求項１０】　通信システムであって：フォーリンネットワークが第一の登録サーバ、第一のアクセスハブおよび第一と第二のインターワーキング機能を含み；ホームネットワークがホーム登録サーバおよび第三のインターワーキング機能を含み、前記フォーリンネットワークは最初はデータフレームを第一のモバイルエンドシステムと前記第一のインターワーキング機能を通じて前記第三のインターワーキング機能との間で通信しており、前記ホームネットワークは最初はデータフレームを前記第三のインターワーキング機能と前記第一の通信サーバとの間で通信しており；前記ホーム登録サーバが第一のモジュールを含み、この第一のモジュールが、登録リクエストが前記第一のモバイルエンドシステムから第一のアクセスポイント、第一のアクセスハブ、および第一の登録サーバを通じて前記ホーム登録サーバに受信されたとき、前記第一のモバイルエンドシステムを前記ホーム登録サーバに、前記第三のインターワーキング機能と前記第一の通信サーバとの間のリンクを切断することなく、再登録し、前記第一のモジュールが、前記登録リクエスト内の前記第一のインターワーキング機能から前記第二のインターワーキング機能への変更を示す指標を認識し；前記ホーム登録サーバがさらに第二のモジュールを含み、この第二のモジュールが、前記第一のモバイルエンドシステムが前記第一のアクセスハブを通じて再登録されたとき、前記第二のインターワーキング機能に対して前記第三のインターワーキング機能とリンクすることを指令し；前記ホーム登録サーバがさらに第三のモジュールを含み、この第三のモジュールが、前記第二のイン

ターワーキング機能が前記第三のインターワーキング機能とリンクされた後に、前記第一のインターワーキング機能に対して前記第三のインターワーキング機能との間のリンクを切断することを指令することを特徴とするシステム。

【請求項１１】　前記フォーリンネットワークが第一のフォーリンネットワークと見なされ、前記第一のフォーリンネットワークがさらに第四のインターワーキング機能を含み；第二のフォーリンネットワークが第二の登録サーバ、第二のアクセスハブおよび第五のインターワーキング機能を含み；前記ホームネットワークがさらに第六のインターワーキング機能を含み、前記第一のフォーリンネットワークは最初はデータフレームを第二のモバイルエンドシステムと前記第四のインターワーキング機能を通じて前記第六のインターワーキング機能との間で通信しており、前記ホームネットワークは最初はデータフレームを前記第六のインターワーキング機能と第二の通信サーバとの間で通信しており；前記ホーム登録サーバがさらに第四のモジュールを含み、この第四のモジュールが、登録リクエストが前記第二のモバイルエンドシステムから第二のアクセスポイント、前記第二のアクセスハブ、および前記第二の登録サーバを通じて前記ホーム登録サーバに受信されたとき、前記第二のモバイルエンドシステムを前記ホーム登録サーバに、前記第六インターワーキング機能と前記第二の通信サーバとの間のリンクを切断することなく、再登録し；前記ホーム登録サーバがさらに第五のモジュールを含み、この第五のモジュールが、前記第二のモバイルエンドシステムが前記第二のアクセスハブを通じて再登録されたとき、前記第五のインターワーキング機能に対して前記第六のインターワーキング機能との間のリンクを切断することを指令し；前記ホーム登録サーバがさらに第六のモジュールを含み、この第六のモジュールが、前記第六のインターワーキング機能が前記第六のインターワーキング機能とリンクされた後に、前記第四のインターワーキング機能に対して前記第六のインターワーキング機能との間のリンクを切断することを指令することを特徴とする請求項１０のシステム。

【請求項１２】　前記フォーリンネットワークが第一のフォーリンネットワークと見なされ、この第一のフォーリンネットワークがさらに第四のインターワーキング機能を含み；第二のフォーリンネットワークが第二の登録サーバ、第二のアクセスハブおよび第五のインターワーキング機能を含み；前記ホームネットワークがさらに第六および第七のインターワーキング機能を含み、前記第一のフォーリンネットワークは最初はデータフレームを第二のモバイルエンドシステムと前記第四のインターワーキング機能を通じて前記第六のインターワーキング機能との間で通信しており、前記ホームネットワークは最初はデータフレームを前記第六のインターワーキング機能と第二の通信サーバとの間で通信しており；前記ホーム登録サーバがさらに第四のモジュールを含み、この第四のモジュールが、登録リクエストが前記第二のモバイルエンドシステムから第二のアクセスポイント、第二のアクセスハブ、および第二の登録サーバを通じて前記ホーム登録サーバに受信されたとき、前記第二のモバイルエンドシステムを前記ホーム登録サーバに再登録し；前記ホーム登録サーバがさらに第五のモジュールを含み、この第五のモジュールが、前記第二のモバイルエンドシステムが前記第二のアクセスハブを通じて再登録されたとき、前記第五のインターワーキング機能に対して前記第七のインターワーキング機能とリンクすることを指令し；前記ホーム登録サーバがさらに第六のモジュールを含み、この第六のモジュールが、前記第七のインターワーキング機能に対して前記第二の通信サーバとリンクすることを指令し；前記ホーム登録サーバがさらに第七のモジュールを含み、この第七のモジュールが、前記第六のインターワーキング機能に対して、前記第二の通信サーバとの間のリンクを切断することを指令し；前記ホーム登録サーバがさらに第八のモジュールを含み、この第八のモジュールが、前記第七のインターワーキング機能が前記第五のインターワーキング機能とリンクされた後に、前記第六のインターワーキング機能に対して前記第四のインターワーキング機能との間のリンクを切断することを指令することを特徴とする請求項１０のシステム。

【請求項１３】　通信システムであって：第一のフォーリンネットワークが第一の登録サーバおよび第一のインターワーキング機能を含み；第二のフォーリンネットワークが第二の登録サーバ、第一のアクセスハブおよび第二のインターワーキング機能を含み；ホームネットワークがホーム登録サーバおよび第三のインターワーキング機能を含み、前記第一のフォーリンネットワークは最初はデータフレームを第一のモバイルエンドシステムと前記第一のインターワーキング機能を通じて前記第三のインターワーキング機能との間で通信しており、前記ホームネットワークは最初はデータフレームを前記第三のインターワーキング機能と前記第一の通信サーバとの間で通信しており；前記ホーム登録サーバが第一のモジュールを含み、この第一のモジュールが、登録リクエストが前記第一のモバイルエンドシステムから第一のアクセスポイント、前記第一のアクセスハブ、および前記第二の登録サーバを通じて前記ホーム登録サーバに受信されたとき、前記第一のモバイルエンドシステムを前記ホーム登録サーバに、前記第三のインターワーキング機能と前記第一の通信サーバとの間のリンクを切断することなく、再登録し；前記ホーム登録サーバがさらに第二のモジュールを含み、この第二のモジュールが、前記第一のモバイルエンドシステムが前記第一のアクセスハブを通じて再登録されたとき、前記第三のインターワーキング

機能に対して前記第二のインターワーキング機能とリンクすることを指令し；前記ホーム登録サーバがさらに第三のモジュールを含み、この第三のモジュールが、前記第三のインターワーキング機能が前記第二のインターワーキング機能とリンクされた後に、前記第三のインターワーキング機能に対して前記第一のインターワーキング機能との間のリンクを切断することを指令することを特徴とする通信システム。

【請求項１４】　通信システムであって：第一のフォーリンネットワークが第一の登録サーバおよび第一のインターワーキング機能を含み；第二のフォーリンネットワークが第二の登録サーバ、第一のアクセスハブおよび第二のインターワーキング機能を含み；ホームネットワークがホーム登録サーバおよび第三と第四のインターワーキング機能を含み、前記第一のフォーリンネットワークは最初はデータフレームを第一のモバイルエンドシステムと前記第一のインターワーキング機能を通じて前記第三のインターワーキング機能との間で通信しており、前記ホームネットワークは最初はデータフレームを前記第三のインターワーキング機能と前記第一の通信サーバとの間で通信しており；前記ホーム登録サーバが第一のモジュールを含み、この第一のモジュールが、登録リクエストが前記第一のモバイルエンドシステムから第一のアクセスポイント、前記第一のアクセスハブおよび前記第二の登録サーバを通じて前記ホーム登録サーバに受信されたとき、前記第一のモバイルエンドシステムを前記ホーム登録サーバに再登録し；前記ホーム登録サーバがさらに第二のモジュールを含み、この第二のモジュールが、前記第一のモバイルエンドシステムが前記第一のアクセスハブを通じて再登録されたとき、前記第四のインターワーキング機能に対して前記第二のインターワーキング機能とリンクすることを指令し；前記ホーム登録サーバがさらに第三のモジュールを含み、この第三のモジュールが、前記第四のインターワーキング機能に対して前記第一の通信サーバとリンクすることを指令し；前記ホーム登録サーバがさらに第四のモジュールを含み、この第四のモジュールが、前記第四のインターワーキング機能が前記第一の通信サーバとリンクされたとき、前記第三のインターワーキング機能に対して前記第一の通信サーバとの間のリンクを切断することを指令し；前記ホーム登録サーバがさらに第五のモジュールを含み、この第五のモジュールが、前記第四のインターワーキング機能が前記第二のインターワーキング機能とリンクされた後に、前記第三のインターワーキング機能に対して前記第一のインターワーキング機能との間のリンクを切断することを指令することを特徴とする通信システム。

【請求項１５】　第一の登録サーバ、第一と第二のアクセスポイントおよび第一のアクセスハブを含むネットワーク内で用いる第一のモバイルエンドシステムと前記第一のアクセスハブとの間の接続をハンドオフする方法であって、この方法が：最初はデータフレームを第一のモバイルエンドシステムと前記第一のアクセスポイントを通じて前記第一のアクセスハブとの間で通信するステップ；前記第一のモバイルエンドシステムが移動し、前記第二のアクセスポイントを通じて再登録するとき、登録リクエストを前記第一のモバイルエンドシステムから前記第二のアクセスポイントを通じて前記第一のアクセスハブに送信することで、前記第一のモバイルエンドシステムを前記第一のアクセスハブに、前記第一の登録サーバに通知することなく、再登録するステップ；前記モバイルエンドシステムが前記第二のアクセスポイントを通じて再登録されたとき、前記第二のアクセスポイントを前記第一アクセスハブにリンクするステップ；および前記第二のアクセスポイントが前記第一のアクセスハブにリンクされたとき、前記第一のアクセスポイントと前記第一のアクセスハブの間のリンクを切断するステップを含むことを特徴とする方法。

【請求項１６】　前記ネットワークがフォーリンネットワークと見なされ、このフォーリンネットワークがさらに第二と第三のアクセスハブおよび第一のインターワーキング機能を含み；ホームネットワークがホーム登録サーバを含み；この方法がさらに、最初にデータフレームを第二のモバイルエンドシステムと第二のアクセスハブを通じて前記第一のインターワーキング機能との間で通信するステップを含み；この方法がさらに、第二のモバイルエンドシステムが移動し、前記第三のアクセスハブを通じて再登録するとき、登録リクエストを第二のモバイルエンドシステムから第三のアクセスポイントおよび第三のアクセスハブを通じて前記第一の登録サーバに送信するとこで、前記第二のモバイルエンドシステムを前記第一の登録サーバに、前記ホーム登録サーバに通知することなく、再登録するステップを含み；この方法がさらに、前記第二のモバイルエンドシステムが前記第三のアクセスハブを通じて再登録されたとき、前記第三のアクセスハブを前記第一のインターワーキング機能とリンクするステップを含み；この方法がさらに、前記第三のアクセスハブと前記第一のインターワーキング機能とがリンクされた後に、前記第二のアクセスハブと前記第一のインターワーキング機能との間のリンクを切断するステップを含むことを特徴とする請求項１５の方法。

【請求項１７】　前記フォーリンネットワークがさらに第四のアクセスハブおよび第二と第三のインターワーキング機能を含み；前記ホームネットワークがさらに第四のインターワーキング機能を含み；この方法がさらに、最初（フォーリンにおいては）データフレームを第三のモバイルエンドシステムと前記第二のインターワーキング機能を通じて前記第四のインターワーキング機能との間で通信するステップを含み；この方法がさらに、最初（ホームにおいては）データフレームを前記第四のインターワーキング機能と第一の通信サーバとの間で通信す

るステップを含み；この方法がさらに、前記第三のモバイルエンドシステムが移動し、前記第四のアクセスハブを通じて再登録するとき、登録リクエストを前記第三のモバイルエンドシステムから第四のアクセスポイント、第四のアクセスハブおよび第一の登録サーバを通じて前記ホームサーバに送信することで、前記第三のモバイルエンドシステムを前記ホーム登録サーバに、前記第四のインターワーキング機能と前記第一の通信サーバとの間のリンクを切断することなく、再登録するステップを含み、この登録リクエストを前記第一の登録サーバから前記ホームサーバに送信するステップが、前記第二のインターワーキング機能から第三のインターワーキング機能への変更を示す指標を送信するサブステップを含み；この方法がさらに、前記第三のモバイルエンドシステムが前記第四のアクセスハブを通じて再登録されたとき、前記第三のインターワーキング機能を前記第四のインターワーキング機能とリンクするステップを含み；この方法がさらに、前記第三のインターワーキング機能が前記第四のインターワーキング機能とリンクされた後に、前記第二のインターワーキング機能と前記第四のインターワーキング機能との間のリンクを切断するステップを含むことを特徴とする請求項１６の方法。

【請求項１８】　前記フォーリンネットワークが第一のフォーリンネットワークと見なされ、この第一のフォーリンネットワークがさらに第五のインターワーキング機能を含み；第二のフォーリンネットワークが第二の登録サーバ、第五のアクセスハブおよび第六のインターワーキング機能を含み；前記ホームネットワークがさらに第七のインターワーキング機能を含み；この方法がさらに、最初（フォーリンにおいては）データフレームを第四のモバイルエンドシステムと前記第五のインターワーキング機能を通じて前記第七のインターワーキング機能との間で通信するステップを含み；この方法がさらに、最初（ホームにおいては）データフレームを第七のインターワーキング機能と第二の通信サーバとの間で通信するステップを含み；この方法がさらに、前記第四のモバイルエンドシステムが移動し、前記第五のアクセスバフを通じて再登録するとき、登録リクエストを前記第四のモバイルエンドシステムから第五のアクセスポイント、第五のアクセスハブおよび第二の登録サーバを通じてホーム登録サーバに送信することで、前記第四のモバイルエンドシステムを前記ホーム登録サーバに、前記第七のインターワーキング機能と前記第二の通信サーバとの間のリンクを切断することなく、再登録するステップを含み；この方法がさらに、前記第四のモバイルエンドシステムが前記第五のアクセスハブを通じて再登録されたとき、前記第六のインターワーキング機能を前記第七ののインターワーキングとリクンするステップを含み；この方法がさらに、前記第六のインターワーキング機能が前記第七のインターワーキング機能とリンクされた後に、前記第六のインターワーキング機能と前記第七のインターワーキング機能との間のリンクを切断するステップを含むことを特徴とする請求項１７の方法。

【請求項１９】　前記フォーリンネットワークが第一のフォーリンネットワークと見なされ、この第一のフォーリンネットワークがさらに第五のインターワーキング機能を含み；第二のフォーリンネットワークが第二の登録サーバ、第五のアクセスハブおよび第六のインターワーキング機能を含み；前記ホームネットワークがさらに第七と第八のインターワーキング機能を含み；この方法がさらに、最初（フォーリンにおいては）データフレームを第四のモバイルエンドシステムと前記第七のインターワーキング機能との間で前記第五のインターワーキング機能を通じて通信するステップを含み；この方法がさらに、最初（ホームにおいては）データフレームを前記第七のインターワーキング機能と第二の通信サーバとの間で通信するステップを含み；この方法がさらに、前記第四のモバイルエンドシステムが移動し、前記第五のアクセスハブを通じて再登録するとき、登録リクエストを前記第四のモバイルエンドシステムから第五のアクセスポイント、前記第五のアクセスハブおよび前記第二の登録サーバを通じて前記ホーム登録サーバに送信することで、前記第四のモバイルエンドシステムを前記ホーム登録サーバに再登録するステップを含み；この方法がさらに、前記第四のモバイルエンドシステムが前記第五のアクセスハブを通じて再登録されたとき、前記第八のインターワーキング機能を前記第六のインターワーキング機能とリンクするステップを含み；この方法がさらに、前記第八のインターワーキング機能を前記第二の通信リンクとリンクするステップを含み；この方法がさらに、前記第七のインターワーキング機能と前記第二の通信サーバとの間のリンクを切断するステップを含み；この方法がさらに、前記第八のインターワーキング機能が前記第六のインターワーキング機能とリンクされた後に、前記第七のインターワーキング機能と前記第五のインターワーキング機能の間のリンクを切断するステップを含むことを特徴とする請求項１９の方法。

【請求項２０】　ホームネットワークがホーム登録サーバを含み、フォーリンネットワークが第一の登録サーバ、第一と第二のアクセスハブおよび第一のインターワーキング機能を含むネットワーク内で用いる第一のモバイルエンドシステムと前記第一のインターワーキング機能との間の接続をハンドオフする方法であって、この方法が：最初は、データフレームを前記第一のモバイルエンドシステムと第一のアクセスハブを通じて前記第一のインターワーキング機能との間で通信するステップ；前記第一のモバイルエンドシステムが移動し、前記第二のアクセスハブを通じて再登録するとき、登録リクエストを前記第一のモバイルエンドシステムから第一のアクセスポイントおよび第二のアクセスハブを通じて前記第一

の登録サーバに送信することで、前記第一のモバイルエンドシステムを前記第一の登録サーバに、前記ホーム登録サーバに通知することなく、再登録するステップ；前記第一のモバイルエンドシステムが前記第二のアクセスハブを通じて再登録されたとき、前記第二のアクセスハブを前記第一のインターワーキング機能とリンクするステップ；および前記第二のアクセスハブが前記第一のインターワーキング機能とリンクされた後に、前記第一のアクセスハブと前記第一のインターワーキング機能との間のリンクを切断するステップを含むことを特徴とする方法。

【請求項２１】　前記フォーリンネットワークがさらに第三のアクセスハブと、第二および第三のインターワーキング機能を含み；前記ホームネットワークがさらに第四のインターワーキング機能を含み；この方法がさらに、最初（フォーリンにおいては）データフレームを第二のモバイルエンドシステムと前記第四のインターワーキング機能との間で前記第二のインターワーキング機能を通じて通信するステップを含み；この方法がさらに、最初（ホームにおいては）データフレームを前記第四のインターワーキング機能と第一の通信サーバとの間で通信するステップを含み；この方法がさらに、前記第二のモバイルエンドシステムが移動し、前記第三のアクセスハブに再登録するとき、登録リクエストを前記第二のモバイルエンドシステムから第二のアクセスポイント、前記第三のアクセスハブおよび前記第一の登録サーバを通じて前記ホーム登録サーバに送信することで、前記第二のモバイルエンドシステムを前記ホーム登録サーバに、前記第四のインターワーキング機能と前記第一の通信サーバとの間のリンクを切断することなく、再登録するステップを含み前記登録リクエストを前記第一の登録サーバから前記ホーム登録サーバに送信するステップが、前記第二のインターワーキング機能から前記第三のインターワーキング機能への変更を示す指標を送信するサブステップを含み；この方法がさらに、前記第二のモバイルエンドシステムが前記第三のアクセスハブを通じて再登録されたとき、前記第三のインターワーキング機能を前記第四のインターワーキング機能にリンクするステップを含み；この方法がさらに、前記第三のインターワーキング機能が前記第四のインターワーキング機能とリンクされた後に、前記第二のインターワーキング機能と前記第四のインターワーキング機能との間のリンクを切断するステップを含むことを特徴とする請求項２０の方法。

【請求項２２】　前記フォーリンネットワークが第一のフォーリンネットワークと見なされ、この第一のフォーリンネットワークがさらに第五のインターワーキング機能を含み；第二のフォーリンネットワークが第二の登録サーバ、第四のアクセスハブおよび第六のインターワーキング機能を含み；前記ホームネットワークがさらに第七のインターワーキング機能を含み；この方法がさらに、最初（フォーリンにおいては）データフレームを第三のモバイルエンドシステムと前記第七のインターワーキング機能との間で前記第五のインターワーキング機能を通じて通信するステップを含み；この方法がさらに、最初（ホームにおいては）データフレームを前記第七のインターワーキング機能と第二の通信サーバとの間で通信するステップを含み；この方法がさらに、前記第三のエンドシステムが前記第四のアクセスハブを通じて再登録するとき、登録リクエストを前記第三のエンドシステムから第三のアクセスポイント、前記第四のアクセスハブおよび前記第二の登録サーバを通じて前記ホーム登録サーバに送信することで、前記第三のモバイルエンドシステムを前記ホーム登録サーバに、前記第七のインターワーキング機能と前記第二の通信サーバとの間のリンクを切断することなく、再登録するステップを含み；この方法がさらに、前記第三のモバイルエンドシステムが前記第四のアクセスハブを通じて再登録されたとき、前記第六のインターワーキング機能を前記第七のインターワーキング機能とリンクするステップを含み；この方法がさらに、前記第六のインターワーキング機能が前記第七のインターワーキング機能とリンクされた後に、前記第五のインターワーキング機能と前記第七のインターワーキング機能との間のリンクを切断するステップを含むことを特徴とする請求項２１の方法。

【請求項２３】　前記フォーリンネットワークが第一のフォーリンネットワークと見なされ、前記第一のフォーリンネットワークがさらに第五のインターワーキング機能を含み；第二のフォーリンネットワークが第二の登録サーバ、第四のアクセスハブおよび第六のインターワーキング機能を含み；前記ホームネットワークがさらに第七および第八のインターワーキング機能を含み；この方法がさらに、最初（フォーリンにおいては）データフレームを第三のモバイルエンドシステムと前記第五のインターワーキング機能を通じて前記第七のインターワーキング機能との間で通信するステップを含み；この方法がさらに、最初（ホームにおいては）データフレームを前記第七のインターワーキング機能と第二の通信サーバとの間で通信するステップを含み；この方法がさらに、前記第三のモバイルエンドシステムが移動し、前記第四のアクセスハブに再登録するとき、登録リクエストを前記第三のモバイルエンドシステムから第三のアクセスポイント、前記第四のアクセスハブおよび前記第二の登録サーバを通じて前記ホーム登録サーバに送信することで、前記第三のモバイルエンドシステムを前記ホーム登録サーバに再登録するステップを含み；この方法がさらに、前記第三のモバイルエンドシステムが前記第四のアクセスハブを通じて再登録されたとき、前記第八のインターワーキング機能を前記第六のインターワーキング機能とリンクするステップを含み；この方法がさらに、前記第八のインターワーキング機能を前記第二の通信サーバと

リンクするステップを含み；この方法がさらに、前記第七のインターワーキング機能と前記第二の通信サーバとの間のリンクを切断するステップを含み；この方法がさらに、前記第八のインターワーキング機能が前記第六のインターワーキング機能とリンクされた後に、前記第七のインターワーキング機能と前記第五のインターワーキング機能との間のリンクを切断するステップを含むことを特徴とする請求項２１の方法。

【請求項２４】　ホームネットワークがホーム登録サーバを含み、フォーリンネットワークが第一の登録サーバ、第一のアクセスハブ、および第一と第二のインターワーキング機能を含み、ホームネットワークがさらに第三のインターワーキング機能を含むネットワーク内で用いる第一のモバイルエンドシステムと第一の通信サーバとの間の接続をハンドオフする方法であって、この方法が：最初（フォーリンにおいては）データフレームを第一のモバイルエンドシステムと前記第一のインターワーキング機能を通じて前記第三のインターワーキング機能との間で通信するステップ；および最初（ホームにおいては）データフレームを前記第三のインターワーキング機能と前記第一の通信サーバとの間で通信するステップ；前記第一のモバイルエンドシステムが移動し、前記第一のアクセスハブを通じて再登録するとき、登録リクエストを前記第一のモバイルエンドシステムから第一のアクセスポイント、第一のアクセスハブおよび第一の登録サーバを通じて前記ホーム登録サーバに送信することで、前記第一のモバイルエンドシステムを前記ホーム登録サーバに、前記第三のインターワーキング機能と前記第一の通信サーバとの間のリンクを切断することなく、再登録するステップを含み；前記登録リクエストを前記第一の登録サーバから前記ホーム登録サーバに送信するステップが、前記第一のインターワーキング機能から前記第二のインターワーキング機能への変更を示す指標を送信するサブステップを含み；この方法がさらに前記第一のモバイルエンドシステムが前記第一のアクセスハブを通じて再登録されたとき、前記第二のインターワーキング機能を前記第三のインターワーキング機能とリンクするステップ；および前記第二のインターワーキング機能が前記第三のインターワーキング機能とリンクされた後に、前記第一のインターワーキング機能と前記第三のインターワーキング機能との間のリンクを切断するステップを含むことを特徴とする方法。

【請求項２５】　前記フォーリンネットワークが第一のフォーリンネットワークと見なされ、前記第一のフォーリンネットワークがさらに第四のインターワーキング機能を含み；第二のフォーリンネットワークが第二の登録サーバ、第二のアクセスハブおよび第五のインターワーキング機能を含み；前記ホームネットワークがさらに第六のインターワーキング機能を含み；この方法がさらに、最初（フォーリンにおいては）データフレームを第二のモバイルエンドシステムと前記第四のインターワーキング機能を通じて前記第六のインターワーキング機能との間で通信するステップを含み；この方法がさらに、最初（ホームにおいては）データフレームを前記第六のインターワーキング機能と第二の通信サーバとの間で通信するステップを含み；この方法がさらに、前記第二の移動エンドシステムが移動し、前記第二のアクセスハブを通じて再登録するとき、登録リクエストを前記第二のモバイルエンドシステムから第二のアクセスポイント、前記第二のアクセスハブ、および前記第二の登録サーバを通じて前記ホーム登録サーバに送信することで、前記第二のモバイルエンドシステムを前記ホーム登録サーバに、前記第六インターワーキング機能と前記第二の通信サーバとの間のリンクを切断することなく、再登録するステップを含み；この方法がさらに、前記第二のモバイルエンドシステムが前記第二のアクセスハブを通じて再登録されたとき、前記第五のインターワーキング機能を前記第六のインターワーキング機能にリンクするステップを含み；この方法がさらに、前記第五のインターワーキング機能が前記第六のインターワーキング機能とリンクされた後に、前記第四のインターワーキング機能と前記第六のインターワーキング機能との間のリンクを切断するステップを含むことを特徴とする請求項２４の方法。

【請求項２６】　前記フォーリンネットワークが第一のフォーリンネットワークと見なされ、この第一のフォーリンネットワークがさらに第四のインターワーキング機能を含み；第二のフォーリンネットワークが第二の登録サーバ、第二のアクセスハブおよび第五のインターワーキング機能を含み；前記ホームネットワークがさらに第六および第七のインターワーキング機能を含み；この方法がさらに、最初（フォーリンにおいては）データフレームを第二のモバイルエンドシステムと前記第四のインターワーキング機能を通じて前記第六のインターワーキング機能との間で通信するステップを含み；この方法がさらに、最初（ホームにおいては）データフレームを前記第六のインターワーキング機能と第二の通信サーバとの間で通信するステップを含み；この方法がさらに、前記第二のモバイルエンドシステムが移動し、前記第二のアクセスハブを通じて再登録するとき、登録リクエストを前記第二のモバイルエンドシステムから第二のアクセスポイント、第二のアクセスハブおよび第二の登録サーバを通じて前記ホーム登録サーバに送信することで、前記第二のモバイルエンドシステムを前記ホーム登録サーバに再登録するステップを含み；この方法さらに、前記第二のモバイルエンドシステムが前記第二のアクセスハブを通じて再登録されたとき、前記第五のインターワーキング機能を前記第七のインターワーキング機能とリンクするステップを含み；この方法がさらに、前記第七のインターワーキング機能を前記第二の通信サーバとリン

クするステップを含み；この方法がさらに、前記第六のインターワーキング機能と前記第二の通信サーバとの間のリンクを切断するステップを含み；この方法がさらに、前記第七のインターワーキング機能が前記第五のインターワーキング機能にリンクされた後に、前記第六のインターワーキング機能と前記第四のインターワーキング機能との間のリンクを切断するステップを含むことを特徴とする請求項２４の方法。

【請求項２７】　ホームネットワークと第一および第二のフォーリンネットワークにおいて用いられる第一のモバイルエンドシステムと第一の通信サーバとの間の接続のハンドオフを行なう方法であって、前記第一のフォーリンネットワークが第一の登録サーバおよび第一のインターワーキング機能を含み、前記第二のフォーリンネットワークが第二の登録サーバ、第一のアクセスハブおよび第二のインターワーキング機能を含み、ホームネットワークがホーム登録サーバおよび第三のインターワーキング機能を含み、この方法が：最初（フォーリンにおいては）データフレームを第一のモバイルエンドシステムと前記第一のインターワーキング機能を通じて前記第三のインターワーキング機能との間で通信するステップ；最初（ホームにおいては）データフレームを前記第三のインターワーキング機能と前記第一の通信サーバとの間で通信するステップ；前記第一のモバイルエンドシステムが移動し、前記第一のアクセスハブを通じて再登録するとき、登録リクエストを前記第一のモバイルエンドシステムから第一のアクセスポイント、前記第一のアクセスハブおよび前記第二の登録サーバを通じて前記ホーム登録サーバに送信することで、前記第一のモバイルエンドシステムを前記ホーム登録サーバに、前記第三のインターワーキング機能と前記第一の通信サーバとの間のリンクを切断することなく、再登録するステップ；前記第一のモバイルエンドシステムが前記第一のアクセスハブを通じて再登録されたとき、前記第三のインターワーキング機能を前記第二のインターワーキング機能とリンクするステップ；および前記第三のインターワーキング機能が前記第二のインターワーキング機能とリンクされた後に、前記第三のインターワーキング機能と前記第一のインターワーキング機能との間のリンクを切断するステップを含むことを特徴とする方法。

【請求項２８】　ホームネットワークと、第一および第二のフォーリンネットワークにおいて用いる第一のモバイルエンドシステムと第一の通信サーバとの間の接続をハンドオフする方法であって、前記第一のフォーリンネットワークが第一の登録サーバおよび第一のインターワーキング機能を含み、前記第二のフォーリンネットワークが第二の登録サーバ、第一のアクセスハブおよび第二のインターワーキング機能を含み、前記ホームネットワークがホーム登録サーバおよび第三と第四のインターワーキング機能を含み、この方法が：最初（フォーリンにおいては）データフレームを第一のモバイルエンドシステムと前記第一のインターワーキング機能を通じて前記第三のインターワーキング機能との間で通信するステップ；最初（フォーリンにおいては）データフレームを前記第三のインターワーキング機能と前記第一の通信サーバとの間で通信するステップ；前記第一のモバイルエンドシステムが移動し、前記第一のアクセスハブを通じて再登録するとき、登録リクエストを前記第一のモバイルエンドシステムから第一のアクセスポイント、前記第一のアクセスハブおよび前記第二の登録サーバを通じて前記ホーム登録サーバに送信することで、前記第一のモバイルエンドシステムを前記ホーム登録サーバに再登録するステップ；前記第一のモバイルエンドシステムが前記第一のアクセスハブを通じて再登録されたとき、前記第四のインターワーキング機能を前記第二のインターワーキング機能にリンクするステップ；前記第四のインターワーキング機能を前記第一の通信サーバにリンクするステップ；前記第四のインターワーキング機能が前記第一の通信サーバにリンクされたとき、前記第三のインターワーキング機能と前記第一の通信サーバとの間のリンクを切断するステップ；および前記第四のインターワーキング機能が前記第二のインターワーキング機能にリンクされた後に、前記第三のインターワーキング機能と前記第一のインターワーキング機能との間のリンクを切断するステップを含むことを特徴とする方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータユーザに、インターネットおよびプライベートイントラネットへのリモートアクセスを仮想プライベートネットワークサービスを用いて高速パケット交換無線データリンクを通じて提供するパケット交換データネットワーク内でのモバイルエンドシステムの管理に関する。本発明は、より詳細には、モバイルエンドシステムがあるセルから別のセルに移動する際のコネクションハンドオーバの管理に関する。

【０００２】

【従来技術】図１は、典型的には一体となってユーザモデム４を通じてユーザコンピュータ２へのリモートインターネットアクセスを提供する３つのビジネスエンティティを示す。第一のビジネスエンティティは、ダイヤルアップ式の簡単な古いタイプの電話システム（plain old telephone system、POTS）あるいはサービス統合データネットワーク（integrated services data network、ISDN）を所有および運用する電話会社である。電話会社は、公衆交換電話ネットワーク（public switched telephone network、PSTN）６の形式にてメディアを提供し、ユーザと他の２つのビジネスエンティティとの間のビット（あるいはパケット）はこの上を流れる。

【０００３】第二のビジネスエンティティは、インター

ネットサービスプロバイダ（ISP）である。ISPは、そのサービスエリア内に一つあるいは複数のポイントオブプレゼンス（point of presence、POP）８を展開および管理し、エンドユーザはネットワークサービスを得るためにここに接続する。ISPは、ISPが顧客の加入を募る主要なローカルコーリングエリア内に、典型的には、一つのPOPを確立する。ＰＯＰは、電話会社によって運用されるＰＳＴＮからのメッセージトラヒックを、ISPによって所有される、あるいはMCI,Inc.等のイントラネットバックボーンプロバイダからリースされるイントラネットバックボーン１０上で運ぶためのデジタル形式に変換する。ISPは、典型的には、PSTNへの接続のために、電話会社からT1ラインの一部もしくわ全部、あるいはT3ラインの一部もしくは全部をリースする。POPとISPのメディアデータセンタ１４は、イントラネットバックボーン上でルータ１２Ａを通じて互いに接続される。データセンタ１４は、IPSのウエブサーバ、メールサーバ、アカウンティングおよび登録サーバを収容し、ISPがウエブコンテント、ｅ－メール、およびウエブホストサービスをエンドユーザに提供することを可能にする。将来の付加価値サービスは、データセンタ内に追加のタイプのサーバを展開することで追加することができる。ISPはさらにルータ１２Ａを公衆インターネットバックボーン２０への接続のために維持する。リモートアクセスに対する現在のモデルにおいては、エンドユーザはユーザの電話会社およびユーザのISPとの間にサービス関係を持ち、通常は両者から別個の請求書を受け取る。エンドユーザは、ISPにアクセスし、ISPから公衆インターネット２０にアクセスするが、これは最寄りのPOPにダイヤルし、インターネット技術標準化委員会（Internet Engineering Task Force、IETE）が勧告するポイトン・ツウ・ポイントプロトコル（point-to point protocol、PPP）として知られる通信プロトコルをランすることで行なう。

【０００４】第三のビジネスエンティティは、事業のために、自身のペライベートイントラネット１８を所有し、これをルータ１２Ｂを通じて運用する私企業である。企業の従業員は自宅あるいは路上から企業イントラネットネットワーク１８にアクセスすることができるが、これはPOTS/ISDN呼を企業のリモートアクセスサーバ１６にかけ、IETF PPPプロトコルをランすることで行なわれる。企業アクセスの場合は、エンドユーザは企業のリモートアクセスサーバ１６に接続するためのコストのみを支払う。この場合はISPは巻き込まれない。私企業は、エンドユーザを企業イントラネット１８、公衆インターネット２０、あるいは両方に接続するためにルータ１２Ｂを維持する。

【０００５】エンドユーザは、電話会社に、電話呼を発信するコストおよび電話回線を自宅に引くコストを支払う。エンドユーザは、さらにISPに、ISPのネットワークにアクセスすることおよびサービスに対してコトスを支払う。本発明は、無線サービスプロバイダ、例えば、Sprint PCS、PrimeCo等、並びに、インターネットサービスプロバイダ、例えば、AOL、AT&T Worldnet等の両方にとって利益である。

【０００６】今日のインターネットサービスプロバイダは、ウエブコンテントサービス、ｅ－メールサービス、コンテントホストサービスおよびローミングサービスをエンドユーザに提供する。マージンの低さや、特徴と価格に基づくマーケットセグメンテーションの展望のなさのために、ISPはマージンを向上するために付加価値サービスを求めている。短期的には、ISPは、設備ベンダによって提供される解決策を用いて、より迅速なアクセス、仮想プライベートネットワーキング（つまり、公衆ネットワークを用いて私設ネットワークと同程度に安全にイントラネットに接続する能力）、ローミングコンソーティアム、プッシュテクノロジー、およびサービス品質を提供することが見込まれる。長期的には、インターネット上での音声や、モビィリティも提供されることが見込まれる。ISPは、低マージンの激戦から脱却するために、これら付加価値サービスを用いることが見込まれる。ところで、これら付加価値サービスの内の多くは、ネットワークサービスの範疇に入るが、これらはネットワークインフラストラクチャ設備を通じてはじめて提供することが可能となる。他の幾つの付加価値サービスは、これもネットワークインフラストラクチャからのサポートを必要とするアプリケーションサービスの範疇に入り、他の幾つかはネットワークインフラストラクチャからのサポートは必要としない。迅速なアクセス、仮想プライベートネットワーキング、ローミング、モビィリティ、サービス品質、サービス品質に基づくアカウンティングは、全て、向上されたネットワークインフラストラクチャを必要とする。発明は、これら向上されたサービスを直接に提供するか、あるいは、将来さらに技術が進歩したときにこれらサービスを追加できるようにするためのフックを提供する。無線サービスプロバイダにとっては、収益奔流の大きなシェアを確保できることが見込まれ、ISPにとっては、より多くのサービス、より良好なマーケットセグメンテーションにて提供できることが見込まれる。

【０００７】

【発明の概要】本発明は、エンドユーザに、公衆インターネット、プライベートイントラネットおよびインターネットサービスプロバイダへのリモート無線アクセスを提供する。無線アクセスがフォーリンネットワーク内の基地局とホームネットワーク内の基地局を通じて両者のインターチエンジ合意の下で提供される。

【０００８】本発明の一つの目的は、モビィリティ管理をローカル、マイクロ、マクロおよびグローバルの４つのコネクションハンドオーバのカテゴリに分割し、これらハンドオーバカテゴリに従ってハンドオフ更新を最小

にするエンドユーザに対する無線パケット交換データネットワークを提供することにある。本発明のもう一つの目的は、MACハンドオフメッセージとネットワークハンドオフメッセージと統合することにある。本発明のさらにもう一つの目的は、別個に、登録機能は登録サーバに、ルーティング機能はインターワーキング機能ユニットに割り当てることにある。本発明のさらにもう一つの目的は、フォーリンネットワーク内の無線ハブ（アクセスハブAHとも呼ばれる）とインターワーキング機能ユニット（IWFユニット）との間に中間XTunnelチャネルを提供することにある。本発明のさらにもう一つの目的は、フォーリンネットワーク内のインターワーキング機能ユニットとホームネットワーク内のインターワーキング機能ユニットとの間にI-XTunnelチャネルを提供することにある。本発明のさらにもう一つの目的は、層２トンネリングプロトコル（layer two tinneling protocol、L2TP）をモバイルエンドシステムがサポートできるように強化することにある。本発明のさらにもう一つの目的は、PPP通信セッションの開始の前にネットワーク層の登録を遂行することにある。本発明を以下に、幾つかの好ましい実施例を図面を参照しながら詳細に説明することで詳細に説明する。

【０００９】

【発明の詳細な記述】本発明は、コンピュータユーザにインターネットやプライベートイントラネットへのリモートアクセスを仮想プライベーサネットワークサービスを用いて高速パケット交換無線データリンクを通じて提供する。これらユーザは、公衆インターネット、プライベートイントラネットあるいはユーザのインターネットサービスプロバイダに無線リンクを通じてアクセスすることができる。ネットワークは、ローミングをサポートする。ここで、ローミングとは、本発明によって提供されるサービスが利用可能な地域であればどこからでもインターネットやプライベートイントラネットに様々な仮想プライベートネットワークサービスを用いてアクセスできる能力を意味する。このネットワークは、水平インターネットやイントラネットアプリケーションをランしているユーザを対象にする。これらアプリケーションには、電子メール、ファイル転送、ブラウザベースのWWWアクセスや、インターネットの周辺に構築されるその他のビジネスアプリケーションが含まれる。このネットワークはIETF標準に準拠するために、このネットワーク上でRTP等のストリーミングメディアプロトコルやH.323等の会議プロトコルをランすることが可能である。

【００１０】既に展開済みあるいは展開の様々な段階にある他のインターネットリモートアクセス技術として、POTSおよびISDNに基づく有線ダイヤルアップアクセス、XDSLアクセス、GSM/CDMA/TDMAに基づく無線回路交換アクセス、ケーブルモデム、衛星ベースのシステム等が含まれる。ただし、本発明による方法は、低い展開コスト、容易な保守、広範な機能セット、スケーラビリティ、重負荷状況におけるグレースフルデグレーション等を特徴とすることに加え、仮想プライベートネットワークキング、ローミング、モビィリティ、ユーザとサービスプロバイダの相対的な利益のためのサービスの品質等の進歩したネットワークサービスをサポートする。

【００１１】パーソナル通信システム（PCS）のスペクトラムを所有する無線サービスプロバイダに対しては、本発明は、プロバイダがPSTNを所有および運用する従来の有線電話会社によって提供されるサービスと十分に競合できる無線パケット交換データアクセスサービスを提供することを可能となる。さらに、プロバイダは、インターネットサービスプロバイダとしても営業することを決意することもできる。この場合は、プロバイダは、ネットワーク全体を所有および運用し、エンド・ツウ・エンドサービスをユーザに提供することとなる。

【００１２】インターネットサービスプロバイダ（internet service providers、ISP）に対しては、本発明はインターネットサービスプロバイダがこのスペクトラムを購入あるいはリースすることを前提に、電話会社をバイパスし、直接に、エンド・ツウ・エンドサービスをユーザに提供することができるようにする。この場合、将来インターネットの普及と共にますます上昇することが見込まれる電話会社へのアクセス料金が節約される。

【００１３】本発明はフレキシブルであり、このため、本発明は、インターネットサービスプロバイダ（ISP）ではなく、単に、エンドユーザに、ISP、インターネットあるいはプライベートイントラネットアクセスを提供する無線サービスプロバイダにとって有益であるばかりか、本発明はさらに、エンドユーザに無線アクセスおよびインターネットサービスを提供するサービスプロバイダにとっても有益である。本発明は、さらに、無線アクセスおよびインターネットサービスを提供するのみでなく、ネットワークの無線部分を他のISPあるいはプライベートイントラネットへのアクセスのために用いることを許すサービスプロバイダにとっても有益である。

【００１４】図２に示すように、エンドシステム３２（例えば、Win 95パーソナルコンピュータに基づく）は無線ネットワーク３０に外部あるいは内部モデムを用いて接続する。これらモデムは、エンドシステムがメディアアクセス制御（medium access control、MAC）フレームをエアリンク３４を通じて送受することを可能にする。外部モデムはＰＣに有線あるいは無線リンクを介して接続される。外部モデムは固定され、例えば、屋根上に搭載される指向性アンテナと同一位置に設置される。外部モデムは、ユーザのＰＣに、以下の手段：つまり、803.2、ユニバーサルシリアルバス、パラレルポート、赤外、さらには、ISM無線リンクの内の任意の一つを用いて接続することができる。内部モデムとしては、好ましくは、ラップトップに対するPCMCIAカードを用い、こ

れがラップトップのバックプレーンに差し込まれる。これらは小型の全指向性アンテナを用いてMACフレームをエアリンクを通じて送受する。

【００１５】広いエリアの無線カバレッジが基地局３６によって提供される。基地局３６によって提供されるカバレッジのレンジは、リンク予算、容量およびカバレッジ等の様々な要因に依存する。基地局は、典型的には、セルサイト内にPSC（パーソナル通信サービス）無線サービスプロバイダによって設置される。基地局は、自身のカバレッジエリア内のエンドシステムから送られるトラヒックを多重化した上で有線回線あるいはマイクロ波バックホールネットワーク３８を通じてシステムのモバイル交換センタ（mobile switching center、MSC）４０に送信する。

【００１６】本発明は、エアリンクのMACとPHY（物理）層およびモデムのタイプに対しては独立である。本発明のアーキテクチャは、バックホールネットワーク３８の物理層およびトポロジに対しても独立である。バックホールネットワークに対する唯一の要件は、バックホールネットワークがインターネットプロトコル（IP）パケットを基地局とMSC（モバイル交換センタ）との間で十分な性能にてルーティングする能力を持つことである。モバイル交換センタ４０（MSC４０）においては、パケットデータインタワーキング機能（IWF）５２がこのネットワークに対する無線プロトコルを終端する。IPルータ４２はMSC４０を公衆インターネット４４、プライベートイントラネット４６あるいはインターネットサービスプロバイダ（ISP）４６に接続する。MSC４０内のアカウンティングおよびディレクトリサーバ４８はアカウンティングデータおよびディレクトリ情報を格納する。エレメント管理サーバ５０は、基地局、IWFおよびアカウンティング／ディレクトリサーバを含む装置を管理する。

【００１７】アカウンティングサーバは、アカウンティングデータをユーザに代わって収集し、このデータをサービスプロバイダの課金システムに送信する。アカウンティングサーバによってサポートされるインタフェースは、アカウンティング情報を、American Management Association（AMA）課金レコードフォーマットにてTCP/IP（transport control protocol/internet protocol：トランスポート制御プロトコル／インターネットプロトコル）トランスポートを通じて課金システム（これも図示せず）に送信する。

【００１８】ネットワークインフラストラクチャプロバイダは、PPP（point-to-point：ポイント・ツウ・ポイントプロトコル）サービスをエンドシステムに提供する。このネットワークは、エンドシステムに対して、（１）ローミングサービス（無線カバレッジが提供されている所ならどこでもログインできるサービス）付きの固定無線アクセス、および（２）低速モビィリティおよびハンドオフサービスを提供する。エンドシステムはネットワークにログオンしたとき、固定サービス（つまり、移動することなく、ハンドオフサービスを必要としないサービス）か、移動サービス（つまり、ハンドオフサービスを必要とするサービス）のいずれかをリクエストする。固定か移動かを指定しないエンドシステムは、移動サービスを指定したものとみなされる。エンドシステムの登録は、実際には、ホーム（オーム）登録サーバと協議して行なわれ、このとき、要求されるサービスのレベル、エンドシステムのユーザによって加入されるサービスのレベル、ネットワーク内の空いた設備等が考慮される。

【００１９】エンドシステムが協議の結果、固定サービス登録（つまり、ハンドサービスを必要としないサービス）を選択し、かつ、エンドシステムがホームネットワーク内に位置する場合は、IWF（インターワーキング機能）が基地局内に実現され、これによってトラヒックがエンドユーザと通信サーバ、例えば、PPPサーバ（つまり、接続されるべきポイント、例えば、ISP PPPサーバ、企業イントラネットPPPサーバ、あるいは無線サービスプロバイダによって顧客に公衆インターネットへの直接のアクセスを提供するために運用されるPPPサーバ等）との間で中継される。メッセージトラヒックの約８０％がこのカテゴリに入ることが見込まれる。つまり、このアーキテクチャは、IWF処理を基地局に分散させることで中央モバイル交換センタ内でメッセージトラヒックが輻湊するのを回避する。

【００２０】他方、エンドシステムが（ホームネットワークあるいはフォーリンネットワークからの）移動サービスをリクエストした場合、あるいは、エンドシステムがローミングサービス（つまり、ホームネットワークからフォーリンネットワークに移動するサービス）を要求した場合は、サービングIWFとホームIWFとの２つのIWFが確立される。サービングIWFは、典型的には、エンドシステムが接続したネットワーク（これはホームネットワークであるかフォーリンネットワークであるかは関係ない）の基地局内に確立され、ホームIWFは、典型的には、ホームネットワークのモバイル交換センタ（MSC）内に確立される。この状況は、メッセージトラヒックの約２０％を占めるのみであるものと見込まれるために、モバイル交換センタにおけるメッセージトラヒックの輻湊は最小限にとどまる。サービングIWFと無線ハブは、コンピュータの同一ネスト内に同一位置に配置あるいは同一のコンピュータ内にプログラムされるために、トンルネルを無線ハブとサービングIWFとの間にXTunnelプロトコルを用いて設定する必要はない。

【００２１】ただし、別の方法として、フォーリンネットワーク内のサービングIWFは、利用可能な設備と要求されるサービスのタイプや品質に基づいて、フォーリンMSC内の設備から選択することもできる。一般的には、ホームIWFがアンカーポイントとなり、これは通信セッ

ションの際に変更されることはなく、サービングIWFの方はエンドシステムが大きく移動すると変更される。

【００２２】基地局は、アクセスハブと少なくとも一つのアクセスポイントを含む（アクセスポイントは、アクセスハブと離して設置することも、同一位置に設置することもできる）。アクセスハブは、典型的には、複数のアクセスポイントを扱う。エンドシステムはアクセスポイントに有線あるいはケーブルによって接続することもできるが、ただし、本発明の一つの好ましい実施例においては、エンドシステムは、アクセスポイントに無線“エアリンク（air link）”によって接続され、この場合、アクセスハブは便宜的に無線ハブと呼ばれる。ここでの説明では、アクセスハブは全般に渡って“無線ハブ（wireless hub）”として示される。ただし、エンドシステムをアクセスポイントを通じてアクセスハブに有線あるいはケーブルを介して接続することも可能であり、この場合は“アクセスハブ（accesshub）”という用語が用いられる。

【００２３】本発明においては、エンドシステムは、エンドユーザ登録エージェント（例えば、エンドシステムのコンピュータ、そのモデム、あるいは両方の上でランするソフトウエア）を含み、これはアクセスポイントと通信、あるいはアクセスポイントを通じて、無線ハブと通信する。無線ハブは、代理（プロキシ）登録エージェント（例えば、無線ハブ内のプロセッサ上でランするソフトウエア）を含み、これはエンドユーザ登録エージェントに対する代理として機能する。この代理登録エージェントと類似する概念が、例えば、IETFによって提唱されるMobile IP標準においては、通常、フォーリンエージェント（foreing agent、FA）と呼ばれている。このため、本発明による代理登録エージェントは、以降、フォーリンエージェントと呼ぶことにし、以下の説明においては、本発明のフォーリンエージェントがIETFによって提唱されるMobile IP標準のフォーリンエージェントと異なる場合にのみの説明する。

【００２４】基地局内に代理登録エージェント（つまり、フォーリンエージェント（FA））を用いることで、エンドシステムのユーザ登録エージェントは、ネットワークへの接続のポイントを見つけ、ホームネットワークのMSC（モバイル交換センタ）内の登録サーバに登録することが可能になる。ホーム登録サーバは、ネットワーク内の複数のインターワーキング機能（IWF）モジュール（実際にはMSCおよび無線ハブの両方の中に設置されたプロセッサ上でランするソフトウエアモジュール）の空き状況を決定し、IWFを登録されたエンドシステムに割り当てる。登録された各エンドシステムに対して、基地局内の無線ハブとモバイル交換センタ（MSC）内のインターワーキング機能（IWF）との間にトンネルが（XTunnelプロトコルを用いて）設定され、このトンネルによって、PPPフレームがエンドシステムとIWFとの間で輸送される。

【００２５】ここで用いられるXTunnelプロトコルとは、PPPデータフレームのシーケンシャルな輸送を提供するフロー制御を備えたプロトコルを意味する。このプロトコルは、標準のIPネットワーク上、ポイント・ツウ・ポイントネットワーク上、あるいはATMデータネットワークやフレームリレーデータネットワーク等の交換式のネットワーク上でランする。これらネットワークは、T1あるいはT3リンクに基づくことも、無線リンクに基づくことも考えられ、さらに、地上ベースであることも、空中ベースであることも考えられる。XTunnelプロトコルは、L2TP（level 2transport protocol）からのアルゴリズムを適応化することによって構築することができる。ただし、データパケットの損失を伴うリンクに基づくネットワークの場合は、再送機能が必須のオプションとなる。

【００２６】エンドシステムのPPPピア（つまり、通信サーバ）は、IWF内あるいは企業イントラネットもしくはISPのネットワーク内に駐在する。PPPピアがIWF内に駐在する場合は、エンドシステムには、直接インターネットアクセスが提供される。PPPピアがイントラネットもしくはISP内に駐在する場合は、エンドシステムには、イントラネットアへのクセスもしくはISPへのアクセスが提供される。イントラネットあるいはISPアクセスをサポートするためには、IWFは、層２トンネルプロトコル（L2TP）を用いて、イントラネットあるいはISPのPPPサーバに接続する。イントラネットあるいはISPのPPPサーバの視点からは、IWFは、ネットワークアクセスサーバ（network access server、NAS）のように見える。エンドシステムとIWFとの間のPPPトラヒックは基地局内のフォーリンエージェントによって中継される。

【００２７】逆（登りリンク）方向の場合は、エンドシステムからIWFに向かうPPPフレームは、MACおよびエアリンクを通じて、基地局に送られる。基地局は、これらフレームを、MSC内のIWFにXTunnelプロトコルを用いて中継する。IWFは処理のためにこれらをPPPサーバに配達する。インターネットアクセスの場合は、PPPサーバは、IWFと同一のマシン内に位置する。ISPあるいはイントラネットアクセスの場合は、PPPサーバはプライベートネットワーク内に位置し、IWFは層２トンネルプロトコル（L2TP）を用いてこれに接続する。

【００２８】順（下りリンク）方向の場合は、PPPサーバからのPPPフレームは、IWFによって基地局にXTunnelプロトコルを用いて中継される。基地局は下りリンクフレームをトンネルから取り出し（デトンネルし）、これをエアリンクを通じてエンドシステムに中継する。次にこのフレームはエンドシステムのPPP層によって処理される。

【００２９】モビィリティ（移動性）をサポートするために、ハンドオフに対するサポートが含まれる。MAC層

は基地局およびエンドシステム内のモビィリティ管理ソフトウエアがハンドオフを効率的に遂行することを支援する。ハンドオフはピアPPPエンティティおよびL2TPトンネルからは透過的に扱われる。エンドシステムが一つの基地局から別の基地局に移動すると、新たなXTunnelが新たな基地局と当初のIWFとの間に生成される。以前の基地局からの以前のXTunnelは削除される。PPPフレームはこの新たな経路を用いて透過的に運ばれる。

【００３０】ネットワークは、ローミング機能（つまり、エンドユーザがフォーリン無線サービスプロバイダを通じて自身のホーム無線サービスプロバイダに接続する機能）をサポートする。この機能を用いると、エンドシステムは、ホームネットワークから離れてフォーリンネットワークにローミングした場合でもサービスを受けることができる。勿論、これは、フォーリン無線サービスプロバイダとエンドシステムのホーム無線サービスプロバイダとがサービス合意を持つことを前提とする。

【００３１】図３は、ローミングエンドシステム６０がフォーリン無線サービスプロバイダ６２がカバレッジを提供する位置まで旅行（ローミング）した状況を示す。ただし、これは、ローミングエンドシステム６０がホーム無線サービスプロバイダ７０と加入者関係を持つことを想定する。さらに、本発明においては、ホーム無線サービスプロバイダ７０がフォーリン無線サービスプロバイダ６２とアクセスサービスを提供する契約関係を持つことを想定する。こうして、図示するように、ローミングエンドシステム６０は、フォーリン無線サービスプロバイダ６２の基地局６４にエアリンクを通じて接続する。次に、データがローミングエンドシステム６０からフォーリン無線サービスプロバイダ６２の基地局６４およびサービングIWF６６を通じてホーム無線サービスプロバイダ７０のホームIWF７２に中継され、場合によっては、さらに、ホーム無線サービスプロバイダ７０のホームIWFを通じてインターネットサービスプロバイダ７４に中継される。

【００３２】ローミングをサポートするためには、I-インタフェースと呼ばれるサービスプロバイダ間インタフェースが無線サービスプロバイダ（wireless service provider、WSP）の境界間の通信のために用いられる。このインタフェースは、認証のため、登録のため、およびエンドシステムのPPPフレームをフォーリンWSPとホームWSPとの間で輸送するために用いられる。

【００３３】PPPフレームは、登りリンク方向と下りリンク方向の両方において、エンドシステムのホーム無線サービスプロバイダ（WSP）を通じて運ばれる。ただし。別の方法として、PPPフレームをフォーリンWSPから直接に宛先ネットワークに輸送することもできる。フォーリンWSP内の基地局はフォーリンネットワークにおけるエンドシステムの接続のポイントである。このフォーリンWSP内の基地局は、PPPフレームをフォーリンWSPのモバイル交換センタ内のサービングIWFに送信、あるいはサービングIWFからPPPフレームを受信する。サービングIWFは、I-インタフェースを通じて、層２トンネルを用いて、ホームIWFと接続し、エンドシステムのPPPフレームを双方向に輸送する。フォーリンWSP内のサービングIWFは監査ためにアカウンティングデータを収集し、ホームWSP内のホームIWFは課金のためにアカウンティングデータを収集する。

【００３４】登録フェーズの際に、フォーリンWSP内の登録サーバはローミングエンドシステムのホームネットワークの識別を調べる（決定する）。フォーリン登録サーバはこの情報を用いてホーム登録サーバと通信し、エンドシステムの認証および登録を行なう。これら登録メッセージはＩ－インタフェースを用いて輸送される。エンドシステムの認証および登録が成功すると、一つの層２トンネルが、基地局とサービングIWFの間にXTUNNELプロトコルを用いて生成され、もう一つの層２トンネルが、サービングIWFとホームIWFの間にＩ－インタフェースを通じて生成される。ホームIWFはエンドシステムのPPPピアに前と同様にL2TP（level 2 tunnelprotocol）を用いて接続する。ハンドオフの際は、ホームIWFの位置とこのL2TPトンネルは固定されたままにとどまる。エンドシステムが一つの基地局からもう一つの基地局に移動すると、新たなトンネルが、新たな基地局とサービングIWFとの間に生成され、以前の基地局とサービングIWFとの間の以前のトンネルは削除される。エンドシステムがさらに遠くまで移動し、新たなサービングIWFが必要になった場合は、新たなトンネルが、新たなサービングIWFとホームIWFとの間に生成され、以前のサービングIWFとホームIWFとの間の以前のトンネルは削除される。

【００３５】ローミングをサポートするために、Ｉ－インタフェースは、認証サービス、登録サービス、および無線サービスプロバイダの境界間でデータを輸送するサービスをサポートする。認証サービスと登録サービスは、IETF Radiusプロトコルを用いてサポートされる。PPPフレームを層２トンネルを通じて輸送するデータ輸送サービスは、I-TXunnelプロトコルを用いてサポートされる。このプロトコルは、IETF L2TPプロトコルに基づく。

【００３６】ここでの説明に用いられるホームIWFという用語は、エンドシステムのホームネットワーク内のIWFを指し、サービングIWFという用語は、フォーリンネットワーク内のエンドシステムに一時的にサービスを提供しているIWFを指す。同様に、ホーム登録サーバという用語は、エンドシステムのホームネットワーク内の登録サーバを指し、フォーリン登録サーバという用語は、エンドシステムがローミングしている最中にそれを通じて登録を行なうフォーリンネットワーク内の登録サーバを指す。

【００３７】ネットワークは、エンドシステムに対し

て、固定と動的の両方のIPアドレス割り当てをサポートする。IPアドレスには、考慮すべき３つのタイプがある。最初の２つのタイプはモバイルIP（mobile IP）と関連し、第三のタイプはPPPと関連する。モバイルIP RFC（mobile IP Request For Comments）は、モバイルIPを用いるエンドシステムは、固定ホームアドレスを持つことを義務付ける。Mobile IPは、また、気付けアドレスをモバイルIPトンネル（本発明の場合はXTunnel）のエンドポイントとして用いることを義務付ける。本発明のネットワークの場合、モバイルIPトンネリング（つまり、XTunnel）に対して用いられる気付けアドレスが基地局のIPアドレスとなる。本発明のネットワークの場合は、固定ホームアドレスは、あえて用いられない。このためモバイルIP登録リクエストパケット（mobile IP registration packets）内では、ホームアドレス欄の値は、0.0.0.0にセットされる。代わりに、構造化されたUser-Name欄が簡略メール転送プロトコル（simplified mail transfer protocol、SMTP）のフォーマットにて、モバイルIP登録リクエストパケットに付加される。これは、user@domainなる形式を持つ。ドメイン（domain）サブ欄は、ユーザのホームドメンイを識別するために用いられ、これは、完全修飾されたドメイン名である。ユーザ（user）サブ欄は、ユーザをホームドメイン内で識別するために用いられる。このUser-Name欄は、エンドシステム上と、MSCの所の加入者データベース内に格納され、これは、ユーザがサービスに加入する際にユーザに割り当てられる。User-Name欄のドメイン（（domain）サブ欄は、ローミングの際に、登録および認証の目的で、ローミング関係と、ホーム登録サーバを識別するために用いられる。

【００３８】PPP IP Configuration Protocol（PPP IPコンフィギュレーションプロトコル）がエンドシステムに対してIPアドレスを協議するために用いられる。IP Configuration Protocol（IPCP）を用いることで、エンドシステムは、固定か動的のいずれかのIPアドレスを協議することができる。

【００３９】上述のように、ホームアドレスは使用せず、代わりに構造化されたUser-Name欄を使用する方法は、本発明が周知のIPと異なる一つの特徴である。ただし、本発明のネットワークは、将来モバイルIPとこれのPPPエンドシステムとの関連での使用がもっと一般化した場合は、User-Name欄は持たず、非零のホームアドレスのみを持つエンドシステムもサポートできるように改良することが考えられる。この場合、サービスロバイダによって、IPCPアドレス割り当てフェーズの際にエンドシステムのホームアドレスと同一のIPアドレスを割り当てるPPPサーバを構成することが考えられる。この場合、ホームアドレスとIPCPによって割り当てられるIPアドレスとは同一となる。

【００４０】図４に示すように、基地局６４とエンドシステムからのエアリンクによって無線サブネットワーク８０が形成され、この無線サブネットワーク８０は、エンドユーザアクセスのためのエアリンク、少なくとも一つの基地局（例えば、基地局６４）、および基地局からMSC４０（図２）に向かう少なくとも一つのバックホールネットワーク（例えば、図２の３８）を含む。例えば、３セクタから成る基地局の無線サブネットワークアーキテクチャは、以下の論理機能を含む。

【００４１】１．アクセスポイント機能（Acess point function）。アクセスポイント８２は、MAC層ブリッジング、並びに、MAC層のアソシエーションとディソシエーション手続きを遂行する。アクセスポイントは、プロセッサ（好ましくは顧客アプリケーションに特化された集積回路（ASIC）の形式）、無線ハブへのリンク（好ましくはカード上のイーサネットリンクあるいはASIC内に組み込まれた形式）、アンテナへのリンク（好ましくはデータ変／復調器と送／受信機を備えるカードの形式）およびアンテナを含み、このアンテナにエンドシステムが結合される。プロセッサは、後に詳細に説明する登録およびモビィリティハンドオーバをサポートするデータブリッジング機能および他の様々な機能を遂行するソフトウエアをランする。これら機能については、後の図７、８、１１の説明の部分を参照されたい。

【００４２】アクセスポイント（AP）は、エアリンクからMAC層のフレームを受け取り、これらを無線ハブに送信、あるいは逆に無線ハブからのフレームをエアリンク（エンドシステム）に送信する。MAC層のアソシエーションとディソシエーション手続きは、APによって、エンドシステムのMACアドレスのリストを自身のMACアドレスフィルタテーブル内に維持するために用いられる。APは、エンドシステムに代わってMAC層ブリッジングを遂行するが、このとき、MACアドレスが自身のMACアドレスフィルタテーブル内に存在するエンドシステムのみが扱われる。アクセスポイントと、それと関連する無線ハブは、典型的には、同一位置に配置される。アクセスポイントは、最も単純な形式においては、単に無線ハブへのポートの形式を取る。APと無線ハブが同一のセルサイト内に同一位置に置かれる場合、これらは、IEEE 802.3リンクを介して互いに接続される。しばしば、アクセスポイントは、無線ハブから離して置かれ、有線T1等のトランク長距離リンクや、場合によっては無線トランクを介して接続される。複数のセクタから成るマルチセクタセルの場合、複数のアクセスポイントが用いられ、各セクタに１つが割り当てられる。

【００４３】２．無線ハブ機能（Wireless hub function）。無線ハブ８４は、フォーリンエージェント（FA）手続き、バックホール負荷のバランシング（例えば複数のT1を使用）、バックホールネットワークインタフェーシング、およびxtunnel手続きを遂行する。サービス品質（QOS）に対するサポートがなされている場合は、無

線ハブは、異なるQOS属性を持つバックホールネットワーク上でxtunnelプロトコルをランすることによって、QOSに対するサポートを実現する。複数のセクタから成るマルチセルサイトの場合は、典型的には、単一の無線ハブ機能が複数のアクセスポイントによって共有される。

【００４４】無線ハブは、プロセッサ、一つのあるいは複数のアクセスポイントへのリンク（好ましくはカード上のイーサネットリンクあるいはASIC内に組み込まれた形式）、およびバックホールへのリンクを含む。バックホールは、典型的には、T1あるいはT3通信回線であり、無線サービスプロバイダのモバイル交換センタに終端する。バックホールへのリンクは、データを、イーサネットフォーマット、フレームリレーフォーマット、あるいはATMフォーマット等の好ましいフォーマットにフォーマット化する。無線ハブプロセッサは、後に詳細に説明するデータブリッジングおよび他の様々な機能をサポートするソフトウエアをランする。これに関しては、後の図９、１０、１１の説明の部分を参照されたい。

【００４５】基地局の設計は、以下のタイプのセルアーキテクチャをサポートする。

１．ローカルAPアーキテクチャ（Local AP architecture）。ローカルAPアーキテクチャの場合は、アクセスポイントは大きな（典型的には２ｋｍ以上）のレンジを持つ。これらは、セルサイト内に、無線ハブと同一位置に配置される（図４）。アクセスポイントは、無線ハブにIEEE 802.3ネットワークを用いて接続することも、無線ハブのバックプレーン内に直接に差し込むことも、あるいは無線ハブに幾つかの他の機構（例えば、ユニバーサルシリアルバス、プリンタポート、赤外線等）を用いて接続することも考えられる。ここでの説明の残りの部分では、第一の代替を用いるものと想定する。セルサイトはオモニ形式にすることも、無線ハブに複数のアクセスポイントとセクタ化されたアンテナを加えることでセクタ化することもできる。

【００４６】２．リモートAPアーキテクチャ（Remote AP architecture）。リモートAPアーキテクチャの場合は、アクセスポイントは、通常は、非常に小さなレンジ、典型的には、半径約１ｋｍのレンジを持つ。これらは、無線ハブから離れて（室内あるいは屋外に）配置される。リモートアクセスポイントは、好ましくは、T1あるいは無線トランクを用いて、無線ハブが位置するセルサイトにリンクされる。セルサイトからは、典型的には、有線のバックホールあるいはマイクロ波リンクを用いて、MSC内のIWFに接続される。リモートAPと無線ハブとの間に無線トランキングが用いられる場合は、トランキングに対してオムニ（全指向性）あるいはセクタ化された無線ラジオが利用される。リモートアクセスポイントへのトランキングのためのデバイスは、好ましくは、無線ハブと同一位置に配置し、これにIEEE 802.3ネットワークを用いて接続するか、あるいは、直接に無線ハブのバックプレーンに差し込む。これらトランキングのためのデバイスは、以降、トランクAPと呼ばれる。

【００４７】３．混合型APアーキテクチャ（Mixed AP architecture）。混合型APアーキテクチャの場合は、無線サブネットワークは、リモートおよびローカルアクセスポイントをサポートする必要がある。ホールフィリングや、他の容量上の理由により複数のリモートアクセスポイントを追加することも考えられる。前述のように、リモートAPは無線ハブにT1あるいは無線トランクを用いて接続される。

【００４８】図５は、ローカルAPのみを用いる３つのセクタを持つセルを示す。アクセスポイントと無線ハブは基地局内に同一位置に配置され、互いに802.3リンクを用いて接続される。

【００４９】図６は、リモートアクセスポイント８２が無線ハブ８４に無線トランク８６を用いて接続されるアーキテクチャを示す。基地局内の各トランクアクセスポイント８６は、リモートマイクロアクセスポイント８２（図面ではR-AP）へのポイント・ツウ・マルチポイント無線ラジオリンクを提供する。リモートアクセスポイントは、エンドシステムに対してエアリンクサービスを提供する。無線ハブとトランクアクセスポイントは基地局内に同一位置に配置され、802.3リンクを介して互いに接続される。この図面には、さらに、ポイント・ツウ・ポイントT1リンクを介して無線ハブに接続されるリモートアクセスポイント８２Ｒも示される。後者のシナリオではトランクAPは必要とされない。

【００５０】上述の全てのセルアーキテクチャ、および各セルによって用いられることが考えられる全ての異なるタイプのアクセスポイントをサポートするためにネットワークアーキテクチャは以下の規則に従う：

【００５１】１．アクセスポイントはMAC層ブリッジとして機能する。リモートアクセスポイントは、エンドシステムへのエアリンクとセルサイトへの無線あるいはT1トランクとの間のMACブリッジングを遂行する。ローカルアクセスポイントは、エンドシステムへのエアリンクと無線ハブとの間のMACブリッジングを遂行する。

２．トランクアクセスポイントもMAC層ブリッジとして機能する。これらはトランク（これはアクセスポイントに向かう）と無線ハブとの間のMACブリッジングを遂行する。

３．無線ハブは全ての同一位置に配置されたMACブリッジ（つまり、ローカルアクセスポイントあるいはトランクアクセスポイント）に最初は802.3リンクを用いて接続する。

【００５２】加えて、T1トランクを備えるローカルアクセスポイントあるいはリモートアクセスポイントが用いられる場合は、以下の規則に従う：

１．ローカルアクセスポイントは、無線ハブと同一位置に配置し、これにポイント・ツウ・ポイント802.3リン

クあるいは共有802.3ネットワークを用いて接続する。第一のアプローチは、アクセスポイントが知能的なMAC層ブリッジング機能を遂行できない場合、あるいは知能的なMAC層ブリッジングでは効率が悪すぎると思われる場合に用いる。リモートアクセスポイントは無線ハブにポイント・ツウ・ポイントT1トランクを用いて接続する。

【００５３】２．セクタ化は、セルサイトにアクセスポイントをセクタ化されたアンテナと共に追加することでサポートする。

３．エンドの登録はモバイルIP技術を用いて行なう。無線アクセスポイントに接続された各アクセスポイントに対して、その無線ハブ内で実行するフォーリンエージェントが存在する。MAC層アソシエーション手続きを用いて、アクセスポイントのMACアドレスフィルタテーブルが最新の状態に維持され、MAC層ブリッジングが効率的に遂行される。無線ハブがMACアソシエーション機能に参加し、正当なMACアドレスのみがアクセスポイントのMACアドレスフィルタテーブルに加えられる。

【００５４】４．無線バブ内のフォーリンエージェントはアクセスポイントからのフレームをMSC IWFに向けて、あるいは逆にMSC IWFからのフレームをアクセスポイントに向けて、xtunnelプロトコルを用いて中継する。MACアドレスフィルタテーブルを用いて、そのMACアドレスがテーブル内に存在しないユニカーストMACデータフレームが除去される。APは、MACブロードキャストフレームとエンドシステムの登録機能と関係するMACフレームについてはMACアドレスフィルタテーブルの内容と関係なく常に中継する。

【００５５】５．ローカルアクセスポイントはIPトラヒックを無線ハブにルーティングするためにARPを用いてMACアドレスを解決する。逆方向において、無線ハブもARPを用いてIPパケットをアクセスポイントにルートする。アクセスポイントのネットワーク管理のためにUDP/IPを用いる。

６．T1を介して接続されたリモートアクセスポイントは、このリンクはポイント・ツウ・ポイントリンクであるためにARPは用いない。

７．ハンドオフに対するサポートにはモバイルIP手続きをMAC層からの支援の下で用いる。

【００５６】無線トランクとトランクAPを用いるセルアーキテクチャでは以下の規則に従う：

１．トランクアクセスポイントは、無線ハブと同一位置に配置され、これにポイント・ツウ・ポイント802.3リンクを用いて接続される。これは、MACフレームのルーティングを簡単にするために行なわれる。共有802.3ネットワークもトランクアクセスポイントがMACブリッジング機能を知能的に遂行できる場合に限り用いることができる。

【００５７】２．無線トランクのセクタ化はセルサイトにトランクアクセスポイントをセクタ化されたアンテナと共に追加することでサポートする。

３．バックホールセクタ間のハンドオフはモバイルIP技術を用いて行う。各バックホールセクタに対して無線ハブ内で実行するフォーリンエージェントが存在する。

４．トランクAPは、MAC層におけるエンドシステムのアソシエーションとハンドオフ手続きに参与する必要はない。これらのMACアドレスフィルタテーブルは、エンドシステムがネットワークに登録すると無線ハブによって動的にプログラムされる。MACアドレスフィルタテーブルを用いてユニカーストMACフレームが除去される。ブロードキャストMACフレームあるいは登録パケットを含むMACフレームについては常に通過することが許される。

【００５８】５．トランクAPは、IPトラヒックを無線ハブにルーティングするためにARPを用いてMACアドレスの解決を行なう。反対方向においては、無線ハブはARPを用いてIPパケットをトランクAPにルートする。UDP/IPがトランクAPのネットワーク管理に用いられる。

【００５９】６．単一無線トランクセクタにおいては、MACアソシエーションと、一つのアクセスポイントから別のアクセスポイントへのハンドオフは、MAC層を用いて行なう。これらMAC層手続きを用いてエンドシステムがアクセスポイントと関連付けられる。エンドシステムが一つのアクセスポイントから別のアクセスポイントに移動すると、アクセスポイントはMACハンドオフプロトコルを用いて自身のMACアドレスフィルタテーブルを更新する。セルサイトの所の無線ハブが、アクセスポイントがこの機能を遂行する際の支援を提供する。この支援には、MAC層ハンドオフメッセージの中継（これはアクセスポイントは直接にMAC層を通じて互いに通信することはできないためである）、MAC層登録およびハンドオフに対するエンドシステムの認証、およびアクセスポイントのMACアドレスフィルタテーブルの更新が含まれる。

【００６０】７．無線トランクセクタに対するフォーリンエージェントがフレームをそのトランクAPからMSCにあるいはこの逆方向にxtunnelプロトコルを用いて中継する責任を持つ。このため、トランクAPに対するフォーリンエージェントは、その無線トランクセクタ内でのエンドシステムのアクセスポイントに関しての位置は感知しない。下りリンク方向においては、このフォーリンエージェントは、単に、モバイルIPトンネルからのフレームを適当なトランクAPに転送するのみであり、このトランクAPがMAC層ブリッジングを用いてこれらフレームをそのバックホールセクタに接続された全てのリモートアクセスポイントに送信する。次に、これらリモートアクセスポイントが自身のMACアドレスフィルタテーブルを調べ、結果に基づいて、そのMACフレームをアクセスネットワーク上に転送、あるいはMACフレームを脱落させ

る。上述のように、MACアドレスフィルタテーブルはMAC層アソシエーションとハンドオフ手続きを用いて最新の状態に維持される。登り方向においては、MACフレームはリモートアクセスポイントによってバックホールブリッジに転送され、バックホールブリッジがこれらを無線ハブ内のフォーリンエージェントに802.3リンクを用いて転送する。

【００６１】８．IPパケットをリモートアクセスポイントに送信あるいはこれから受信するためにARPは用いない。リモートアクセスポイントは無線ハブのMACアドレスをBOOTP手続きを用いて決定する。逆に、無線ハブはリモートアクセスポイントのMACアドレスを用いて構成される。アクセスポイントのネットワークネットワーク管理、およびエンドシステムのアソシエーションとハンドオフメッセージにはUDP/IPを用いる。セルサイト内のIEEE 802.3リンクはより高速のリンクと交換することもできる。

【００６２】図７は、ローカルアクセスポイントのプロトコルスタックを示す。このスタックのベースには物理層PHYが存在する。物理層PHYは、データをエンドシステムとの間で送信あるいは受信する。これらデータはストリームにてデータ変調器に送信あるいは復調器から受信される。APがエンドシステムからのデータを物理層を通じて受信した場合は、APは、これをMACフレーム（MAC層）にアンパックする。次に、このMACフレームは、イーサネット物理層フォーマット（IEEE 802.3フォーマット）に再パックされ、イーサネットリンクを介して無線ハブに送信される。逆に、APのプロセッサがエンドシステムに伝送されるべきデータを無線ハブからイーサネットリンク（つまり、物理リンク）を介して受信した場合は、APは、そのデータをメディアアクセス制御（MAC）フォーマットにパックし、次に、このMAC層データを変調器に送信する。次に、変調器がこのデータをエンドシステムに送信する。

【００６３】図８においては、図７に示すエンドシステムに向かう／あるいはこれからのMAC層とPHY層が、セルサイトへのトランクに対するリモートアクセスポイントのMAC層とPHY層と置換される。T1トランク上では、好ましくは、ハイレベルデータリンクプロトコル（high level data link protocol、HDLCプロトコル）を用いる。

図９は、バックホールとエンドアクセスポイントへのトランクをブリッジする無線ハブのプロトコルスタックを示す。リモートAPへのトランクはリモートアクセスポイントのサポートのみに要求される（これとは対照的にイーサネットはアクセスポイントを接続する）。リモートAPへの無線トランクのMAC層とPHY層は、ポイント・ツウ・マルチポイントリンクを提供し、一つのトランクが同一セクタ内の複数のリモートAPと通信するために用いられる。

【００６４】無線ハブはリモートAPへのトランクとネットワークのモバイル交換センタ（MSC）へのバックホール（例えば、T1あるいはT3）をブリッジする。無線ハブ内のプロトコルスタックは、MSCへのMAC層とPHY層を実現し、この上部にはIP（Internet Protocol）層が実現され、さらにこの上部にはネットワーク管理のためのUDP（Universal Datagram Protocol）層が実現され（IP層とUDP層は組み合わせてUDP/IPと呼ばれる）、さらにこの上部にはXTunnelプロトコルが実現される。XTunnelプロトコルは新たなフォーマットであり、提唱されているIETF Mobile IP標準の特徴とLevel 2 Tunnel Protocol（L2TP）の特徴の両方を含む。XTunnelプロトコルは、無線ハブからMSCへの通信、および、異なるネットワークあるいは同一ネットワーク内のインターワーキング機能（IWF）間の通信のために用いられる。

【００６５】図１０はリモートアクセスポイントをサポートするための基地局内のリレー機能のプロトコルスタックを示す。このリレー機能には、バックホールへのインタフェース（無線ハブとして示す）とリモートAPへのインタフェース（トランクAPとして示す）が含まれる。無線ハブの観点からは、（図７と図１０に示す）トランクAPは、実際には、図７に示すAPのように振る舞う。好ましくは、基地局のプロトコルスタックは、無線ハブとトランクAPに分割され、この間をイーサネットによって接続される。Ｎ個のセクタから成る無線トランクの場合は、セルサイト内のＮ個の無線トランクAPと１個の無線ハブが存在する。

【００６６】図１１はローカルAPを用いるセルアーキテクチャの基地局のプロトコルスタックを示す。リレー機能には、バックホールへのインタフェース（無線ハブとして示す）とエンドシステムへのエアリンクインタフェース（APとして示す）が含まれる。無線ハブの観点からは、（図８と図１１に示す）APは、実際には図８に示すトランクAPのように振る舞う。好ましくは、基地局のプロトコルスタックは、無線ハブとトランクAPとの分割され、これらがイーサネットによって接続される。Ｎ個のセクタから成るセルの場合は、Ｎ個のアクセスポイントと１個の無線ハブが存在する。

【００６７】基地局からMSCへのバックホールネットワークは以下の属性を持つ：

１．このネットワークはIPデータグラムを基地局とMSCとの間でルーティングする能力を持つ。

２．このネットワークはセキュリティである。これは、公衆インターネットではない。このネットワークはエンドシステムのトラヒックを輸送するためのみでなく、認証、アカウンティング、登録、および管理トラヒックも輸送するために、信託された（トラストされた）ノードからのトラヒックのみがこのネットワーク上に入ることを許される。

３．このネットワークは必要な性能特性を備える。

【００６８】典型的なアプリケーションにおいてはサー

ビスプロバイダはその上に装置を設置するバックホールネットワークを設置および維持する責任を持つ。基地局はMSCと通信するために、以下のバックホールインタフェースをサポートする：

１．基地局は、IP over PPP with HDLC link（IETF標準）をポイント・ツウ・ポイントT1リンクあるいはT3リンクの一部分を用いてサポートる。

２．基地局は、IP over frame relay（IETF標準）をT1リンクあるいはT3リンクの一部分を用いてサポートする。

３．基地局は、IP over AAL5/ATM（IETF標準）をT1リンクあるいはT3リンクの一部分を用いてサポートする。

【００６９】上述のインタフェースは全てIETF標準のカプセル化に基づくため、MSC内に市販のルータを用いてこのバックホールネットワークの物理リンクを終端することができる。より上位の層は、様々なサーバや他のプロセッサにパスされ、そこで処理される。

【００７０】MAC層の上部のエンドシステム登録手続きがサポートされる。以下の説明ではMAC層の所のエンドシステム登録手続きは、上位の層に影響を与えない限り無視される。

【００７１】エンドシステムはサービスを求めてホームネットワークからあるいはフォーリンネットワークから登録する。両方のシナリオにおいて、エンドシステムは基地局内のフォーリンエージェント（FA）を用いて、登録のためのネットワークへの接続ポイントを見つける。前者の場合、FAはエンドシステムのホームネットワーク内に存在し、後者の場合、FAはフォーリンネットワーク内に存在する。いずれの場合も、ネットワークはエンドシステムのホームネットワーク内のIWFをアンカーポイント（つまり、移動してもセッションを通じて変更されないポイント）として用いる。エンドシステムへのあるいはこれからのPPPフレームは、基地局内のFAを介してホームネットワーク内のIWFに送られる。エンドシステムがホームにる場合は、ホームIWFが直接にxtunnelプロトコルを介してに基地局に接続される。エンドシステムがフォーリンにローミングしている場合は、フォーリンネットワーク内のサービングIWFがホームIWFにＩ－インタフェースを通じて接続される。サービングIWFは基地局とホームIWFとの間でフレームを中継する。ホームIWFからは、データは、同一のIWF内に駐在するPPPサーバに送られることも、別個のサーバにL2TPを用いて送られることもある。別個のサーバは無線サービスプロバイダとは異なるプライベートネットワークオペレータ（例えば、ISPあるいは企業イントラネット）によって所有および運用される。このセッションの最中、ホームIWFとPPPサーバの位置は固定されたままにとどまる。エンドシステムが接続した状態で移動した場合、これは、新たなフォーリンエージェントに再登録することが必要となる。ただし、同一のIWFとPPPサーバが引き続いて用いられる。新たなFAとIWFとの間に新たなxtunnelが生成され、以前のフォーリンエージェントとIFWとの間の以前のxtunnelは削除される。

【００７２】図１２は、２つのエンドシステムＡ、Ｂに対するこのネットワークの第一の構成（コンフィギュレーション）を示す。ここでは、これらエンドシステムの両方のホーム無線ネットワークは無線サービスプロバイダＡ（WSP-A）である。一方のエンドシステムはホーム無線ネットワークから登録し、他方のエンドシステムはフォーリン無線ネットワークから登録する。WSP-A内のホームIWFが両方のエンドシステムに対するアンカーポイントとして機能する。両方のエンドシステムについて、データはホームIWFに中継される。ホームIWFはISP-Aによって所有されるインターネットサービスプロバイダのPPPに接続する。ここでは、両方のエンドシステムが同一のISPに加入しているものと想定する。ただし、別のISPに加入している場合は、ホームIWFは別のISPにも接続される。

【００７３】無線サービスプロバイダのネットワーク内部においては、基地局とIWFの間ではデータはxtunnelプロトコルを用いて運ばれる。IWFとPPPサーバの間ではデータはLevel 2 Tunneling Protocol（L2TP）を用いて運ばれる。サービングIWFとホームIWFとの間では、データはI-xtunnelプロトコルを用いて運ばれる。

【００７４】常にホームネットワーク内のIWFを用いることには長所と短所がある。最も明らかな長所は単純なことである。短所は、常に、リモートのホームIWFとの間でデータを中継することが必要になることである。代替として、サービングIWFによってエンドシステムのISP／イントラネットに接続するために必要とされる全ての情報をサービングIWFに送信し、サービングIWFがアカウンティング情報をリアルタイムにてホームネットワーク内のアカウンティングサーバに送り返す方法も考えられる。この機能は実現はより困難であるが、データをフォーリンネットワークからホームネットワークに長距離に渡って中継する必要性が低減されるために効率は良くなる。

【００７５】例えば、シカゴから香港にローミングするユーザのケースについて考える。ユーザのホームネットワークがシカゴに存在し、ユーザが香港内の無線サービスプロバイダを用いて登録するものと想定する。この場合、第一の構成では、アンカーポイントはシカゴ内のホームIWFとなり、全てのデータを香港とシカゴり間で中継することが必要となる。シカゴ内のホームIWFはシカゴ内のユーザのIPSに接続する。これに対して第二の構成では、エンドシステムのユーザには香港内のISPが割り当てられる。このために、データをシカゴと香港の間で常に中継する必要はなくなる。第二の構成では、サービングIWFがアンカーとして機能し、サービングIWFはエンドシステムが移動した場合でもセッションを通じて変

更されない。ただし、FAの位置はエンドシステムが香港内で移動すると変更される。

【００７６】図１３は、第二のネットワーク構成を示す。この図面では、エンドシステムＡ、Ｂに対するホームネットワークはWSP-Aである。エンドシステムＡは、ホームネットワークから登録し、ホームIWFをアンカーポイントとして用い、また、ISP-AにISPのPPPサーバを用いて接続する。エンドシステムＢの方は、WSP-Bのフォーリンネットワークから登録し、サービングIWFを用いる。このサービングIWFは、アンカーポイントとして機能するとともに、エンドシステムをISPにISPのＰＰＰサーバを用いて接続する。この構成では、エンドシステムＢのデータはフォーリンネットワークとホームネットワークの間を中継する必要はなくなる。

【００７７】この構成が機能するためには、ホームとフォーリンの無線サービスプロバイダの間にローミング合意があるのみでなく、フォーリン無線サービスプロバイダとエンドシステムのインターネットサービスプロバイダとの間にも、直接にあるいは仲介者を通じて、合意があることが必要となる。上述の例では、香港内の無線サービスプロバイダとシカゴ内の無線サービスプロバイダがビジネス合意を持つことに加えて、香港内のＷＳＰが、エンドシステム（ユーザ）のChcago ISPとの間に、香港内のChcago ISPのPPPサーバにアクセスすることに関するビジネス合意を持つか、あるいは、ユーザのChcago ISPとの間にローミングに関するビジネス合意を持つ香港内に位置する他のISPとの間にビジネス合意を持つことを要求される。加えて、香港内のWSPは、ユーザの認証、アカウンティング、適当なトンネルの設定等を遂行するためにこれらのローミング関係を動的に発見できることを要求される。

【００７８】インターネットインフラストラクチャ事業に従事する様々な企業が、IETF（インターネット技術標準化委員会）において、適当な基準をこれら全てのシナリオに対して策定するまでには、まだ時間がかかると思われる。このため、現時点では、前者のより単純なホームネットワーク内のIWFが常にアンカー点として用いられる構成が、多少効率は落ちるが、本発明の好ましい実施例とされる。ただし、インターネットローミングに対するプロトコルの適当な産業標準が策定された暁には第二の構成についても同等なあるいは代替の実施例として考慮されるべきである。

【００７９】エンドシステムは、PPPを開始しデータを送受するためには、その前に、無線ネットワークに登録する必要がある。このため、エンドシステムは、最初に、FAの発見と登録のフェーズに入る。これらフェーズを通じてエンドシステムが認証され、無線サービスプロバイダに登録される。これらフェーズが終了すると、エンドシステムはPPPを開始する。これには、PPPリンク設定フェーズ、PPP認証フェーズ、およびPPPネットワーク制御プロトコルフェーズが含まれる。いったんこれらフェーズが終了すると、エンドシステムはPPPを用いてIPパケットを送受することが可能になる。

【００８０】以下の説明においては、エンドシステムがフォーリンにローミングしており、フォーリンネットワークから登録するものと想定する。FA発見フェーズにおいて、エンドシステムは（自身のユーザ登録エージェントを通じて）フォーリンエージェントからのアドバタイズメントを要請する。ユーザ登録エージェントは付近のフォーリンエージェントによって送信されたアドバタイズメントメッセージ（advertisement messages）を用いて、登録のためのFAの識別を見つる。登録フェーズにおいて、エンドシステムのユーザ登録エージェントは、FAの気付けアドレスを選択し、そのアドレスに向けて登録リクエストを送る。FAは、代理（プロキシ）登録エージェントとして機能し、この登録リクエストをフォーリン登録サーバ（フォーリンWSP内の登録サーバ）に転送する。フォーリン登録サーバは、ユーザ登録エージェントのリクエスト内のUser-Name欄を用いて、エンドシステムのホームネットワークを調べ、この登録リクエストを、認証のために、ホームネットワーク内の登録サーバに転送する。ホーム登録サーバはフォーリン登録サーバによって中継された登録リクエストを受信すると、フォーリン登録サーバの識別とエンドシステムの識別の認証を行なう。認証と登録が成功すると、ホーム登録サーバはホームネットワーク内のIWFを選択し、ホームIWFと（フォーリンWSP内の）サービングIWFとの間にI-xtunnelリンクを生成する。ホームネットワーク内のIWFは、このPPPセッションを通じて終始アンカー点として機能する。

【００８１】いったんモービルIP（mobile IP）の認証および登録フェーズが終了すると、様々なPPPフェーズが開始される。PPPの開始時に、ホームIWFと要求されたISP／イントラネットPPPサーバとの間にL2TP接続が生成される。PPP認証フェーズにおいては、PPPパスワードがPAPあるいはCHAPを用いて交換され、ISPあるいはイントラネットPPPサーバは独自にエンドシステムの識別の認証を行なう。

【００８２】いったんこれが成功すると、PPPネットワーク制御フェーズが開始される。このフェーズにおいては、IPアドレスが協議され、IPアドレスがPPPサーバによってエンドシステムに割り当てられ、TCP/IP見出しの圧縮の使用についても協議される。これが終了すると、エンドシステムは、自身のISPあるいは企業イントラネットとの間でIPパケットをPPPを用いて送受することが可能になる。

【００８３】認証が２つのレベルで遂行されることに注意する。モービルIPの認証においては、エンドシステムの識別がホームネットワーク内のホーム登録サーバと比較され、さらに、フォーリンネットワークの識別とホー

ムネットワークの識別が互いに比較される。この機能を遂行するために、フォーリンエージェントは、エンドシステムの登録リクエストを、例えば、IETE Radiusプロトコルを用いて自身のローカルMSC内のフォーリン登録サーバにRadius Aceess-Requestパケットに入れて送信する。フォーリン登録サーバはエンドシステムのドメイン名を用いてエンドシステムのホームネットワークとホーム登録サーバの識別を決定し、Radius代理として機能することで、このリクエストをカプセル化し、エンドシステムのホーム登録サーバに転送する。一方、フォーリン登録サーバがエンドシステムのホームネットワークの識別を決定できない場合は、フォーリン登録サーバは、オプションとして、Radiusリクエストを、ブローカのように機能する登録サーバ（例えば、無線サービスプロバイダの協会によって所有される登録サーバ）に転送することもできる。この場合は、このブローカが代わって、Radius Aceess-Requestを最終的なホーム登録サーバに送る。このローカル登録サーバが、その登録リクエストをローカル的にあるいは代理として扱うことができない場合は、ローカル登録サーバはそのフォーリンエージェントの登録リクエストを拒絶し、次に、フォーリンエージェントがエンドシステムの登録リクエストを拒絶する。他方、ホーム登録サーバは、Radius Access-Requestを受信すると、フォーリンネットワークとエンドシステムの識別について必要な認証を遂行する。認証と登録が成功すると、ホーム登録サーバは、Radius Access-Responseパケットをフォーリン登録サーバに送り返し、次に、フォーリン登録サーバが応答をフォーリンエージェントに送り、こうして、ラウンドトリップ（一巡）が完了する。登録リクエストは、ホームサーバがなんらかの理由で受諾しない場合は拒絶される。

【００８４】第二のレベルに認証動作においては、エンドシステムの識別がイントラネットあるいはISPのPPPサーバと比較される。モビリティ認証とは別個にPPP認証を行なうことで、インフラストラクチャ設備をISPとは別個に展開および所有するこが可能になる。

【００８５】図１４は、ローミングエンドシステムに対する登録シーケンスを示す梯子図である。PPPサーバとホームIWFは同一サーバ内に位置し、L2TPは必要ないものと想定する。登録エンドシステムに代わってアカウンティングを開始するために行なわれるアカウンティングサーバとの対話、並びにホーム登録サーバの識別を決定するためおよびエンドシステムの識別を認証するためのディレクトリサーバとの対話についても示される。ただし、アカウンティング、課金、（サービスプロバイダ間の）ローミング、および清算に関しては後に説明する。

【００８６】エンドシステムのユーザ登録エージェントからのMAC層メッセージ（例えば、802.11ビーコン）によって、Agent Solicitationが開始される。MAC層のメッセージは、図面を簡潔化するために示されていない。

【００８７】図１４に示すように、最初に、エンドシステム（モバイル）がアドバタイズメントを要請し、フォーリンエージェントがアドバタイズメントを送り返す。エンドシステムは、このアドバタイズメントからフォーリンエージェントが属するネットワークに関する情報を知る。この情報には、フォーリンエージェントの気付けアドレスも含まれる。ここでの説明においては、このネットワークはフォーリン無線サービスプロバイダであるものと想定する。次に、エンドシステム内のユーザ登録エージェントが、フォーリンエージェントとそのネットワークに関する情報（気付けアドレスも含め）を登録リクエストに組み入れ、この登録リクエストをフォーリンエージェントに送る。このフォーリンエージェントは、代理（プロキシ）登録エージェントとして機能し、登録リクエストをフォーリン登録サーバ（つまり、フォーリン無線サービスプロバイダの登録サーバ）に中継する。すると、フォーリン登録サーバは、そのリクエストがホームディレクトリではないことを認識し、フォーリンディレクトリサーバにアクセスする。フォーリンディレクトリサーバはフォーリン無線サービスプロバイダのFDD（フォーリンドメインディレクトリ）を用いて、その登録リクエストをエンドシステムが属する無線サービスプロバイダのホーム登録サーバにどのようにして送信すれば良いか調べ、次に、この転送のために必要な情報をフォーリン登録サーバに送り返す。次に、フォーリン登録サーバは、エンドシステムの登録リクエストをRadiusアクセスリクエスト内にカプセル化し（組み入れ）、このカプセル化したリクエストを、そのエンドシステムが属する無線サービスプロバイダのホーム登録サーバに中継する。すると、ホーム登録サーバはホームディレクトリサーバにアクセスし、ホームディレクトリサーバは、ホーム登録サーバのHDDを用いて少なくともフォーリンサービスプロバイダについての認証情報を調べ、これをホーム登録サーバに送り返す。オプションとして、ホーム登録サーバは、加入者のディレクトリにアクセスすることで、詳細な加入者サービスプロフィル情報（例えば、加入しているサービスオプションの品質等）を得ることもできる。結果として、全てのパーティが認証されると、ホーム登録サーバはホームIWFとPPPサーバにstart IWF request（IWF開始リクエスト）を送信する。ホームIWFとPPPサーバはホームアカウンティングサーバを始動し、その後、start IWF response（開始確認応答）をホーム登録サーバに送り返す。すると、ホーム登録サーバは、Radius access response（Radiusアクセス確認応答）をフォーリン登録サーバに送る。次に、フォーリン登録サーバは、start IWF request（IWF開始リクエスト）Iをサービング IWFに送る。サービングIWFは、サービングアカウンティングサーバを始動し、その後、start IWF response（開始確認応答）Iをフォーリン登録サーバに送り返す。フォーリン登録サーバは登録応答をフ

ォーリンエージェントに送り、フォーリンエージェントはこの登録応答をエンドシステムに中継する。

【００８８】次に、エンドシステムが、リンク制御プロトコル（link control protocol、LCP）コンフィギュレーションリクエストを、フォーリン登録サーバを通じて、ホームIWFとPPPサーバに送る。すると、ホームIWFとPPPサーバは、LCPコンフィギュレーション確認応答を、フォーリン登録サーバを通じて、エンドシステムに送り返す。

【００８９】次に、エンドシステムは、同様に、パスワード認証プロトコル（password authentication protocol、PAP）認証リクエストをホームIWFとPPPサーバに送り、ホームIWFとPPPサーバは、PAP確認応答をエンドシステムに返す。別の方法として、認証のためにchallenge authentication protocol（CHAP）（認証挑戦プロトコル）を用いることもできる。認証のために両方のプロトコルを用いることも、このフェーズはスキップすることもできる。

【００９０】次に、エンドシステムは、同様に、IPコンフィギュレーションプロトコル（IPconfiguration protocol、IPCP）をホームIWFとPPPサーバに送り、ホームIWFとPPPサーバはPCP確認応答を送り返す。エンドシステムへの接続は以下の理由の任意の一つによって終端される。

【００９１】１．ユーザ始動の終端。このシナリオの下では、エンドシステムが最初にPPPをグレースフルに終端させる。これには、PPPネットワーク制御プロトコル（IPCP）の終端と、これに続く、PPPリンクプロトコルの終端が含まれる。いったんこれが行なわれると、エンドシステムのネットワークへの登録が解除され、続いて、アクセスポイントへの無線リンクが終端される。

【００９２】２．無線リンクの損失。このシナリオはエンドシステム内のモデムによって検出され、モデムドライバに報告される。すると、ソフトウエアの上位層にスタックを終端する通告が送られ、終端がユーザに通知される。

３．フォーリンエージェントへの接続の損失。このシナリオは、エンドシステム内のモビリィティドライバによって検出される。（潜在的に新たな）フォーリンエージェントとコンタクトすることを再び試み、失敗した場合は、ドライバは、適当な通知を上位のプロトコルスタックに送り、同時に、下位のモデムに信号を送り、無線リンクを終端させる。

【００９３】４．IWFへの接続の損失。これは、フォーリンエージェントへの接続が失われた場合と実質的に同一である。

５．IWFあるいはPPPサーバによるPPPの終端。このシナリオは、エンドシステム内のPPPソフトウエアによって検出され、エンドシステムのPPPドライバにこの事象が通知される。PPPドライバは、ネットワークへの登録の解除を試み、続いて、アクセスポイントへの無線リンクを終端する。

【００９４】エンドシステムのサービスコンフィギュレーションとは、ネットワークサービスをエンドシステムに対して加入者のサービスプロフィルに基づいて構成する概念を意味する。加入者のサービスプロフィルは、加入者ディレクトリ内に格納されている。ソフトウエアは、このサービスプロフィルに含まれる情報を用いて、無線データサービスを加入者に代わってカスタム化する。この情報には、エンドシステムの認証、エンドシステムのローミング、エンドシステムのインターネットサービスプロバイダへの接続の設定等に用いる情報が含まれる。この情報には、さらに、好ましくは、サービスの品質等の他のパラメータも含まれる。加入者ディレクトリに加え、ホームドメインディレクトリ（HDD）とフォーリンドメインディレクトリ（FDD）がローミングおよびフォーリン登録サーバとホーム登録サーバを互いに認証するために用いられる。HDDは、エンドシステムのホームネットワークに関する情報を格納し、FDDは、加入者が訪問するフォーリンネットワークに関する情報を格納する。

【００９５】図１５は、これらディレクトリがいかにネットワークアーキテクチャにマッピングされ、これらがホームから登録するエンドシステムに対して登録の際にいかに用いられるかを示す。ステップ０において、エンドシステム（モバイル）がアドバタイズメントを要請し、フォーリンエージェントがアドバタイズメントを介してエンドシステムにそのフォーリンエージェントが属するネットワークに関する情報を供給する。このケースにおいては、このネットワークはホーム無線サービスプロバイダであるものと想定される。ステップ１において、エンドシステム内のユーザ登録エージェントが、こうして得られたフォーリンエージェントとそのネットワークに関する情報をリクエスト内に組み入れ、このリクエストをフォーリンエージェントに送信する。ステップ２において、フォーリンエージェントが、代理登録エージェントとして、このリクエストをホーム登録サーバに中継する。ステップ３において、ホーム登録サーバが、ホーム無線サービスプロバイダのHDDにアクセスすることで、少なくとも認証情報を得る。ステップ４において、ホーム登録サーバは、さらに、加入者ディレクトリにアクセスすることで、詳細な加入者サービスプロフィル情報（例えば、加入されるサービスオプションの品質等）を得る。ステップ５において、ホーム登録サーバがフォーリンエージェントにアクセス確認応答を送り返す。ステップ６と７において、フォーリンエージェントがエンドシステム（つまり、モバイル）に登録の確認応答を送り返す。

【００９６】図１６は、フォーリンネットワークから登録するエンドシステムに対するディレクトリの使用を示

す。ステップ０において、エンドシステム（モバイル）がアドバタイズメントを要請し、フォーリンエージェントがアドバタイズメントを介して、エンドシステムに、そのフォーリンエージェントが属するネットワークに関する情報を供給する。このケースにおいては、このネットワークは、フォーリン無線サービスプロバイダであるものと想定される。ステップ１において、エンドシステム内のユーザ登録エージェントが、フォーリンエージェントとそのネットワークに関する情報をリクエスト内に組み入れ、このリクエストをフォーリンエージェントに送信する。ステップ２において、フォーリンエージェントが、代理登録エージェントとして、このリクエストをフォーリン登録サーバ（つまり、フォーリン無線サービスプロバイダの登録サーバ）に中継する。ステップ３において、フォーリン登録サーバがフォーリン無線サービスプロバイダのHDDにアクセスすることで、エンドシステムが属するネットワークの情報を得る。ステップ４において、フォーリン登録サーバが、エンドシステムのリクエストを、エンドシステムのホーム無線サービスプロバイダのホーム登録サーバに転送する。ステップ５において、ホーム登録サーバがホーム登録サーバのFDDにアクセスし、少なくともフォーリンサービスプロバイダに関する認証情報を得る。ステップ６において、ホーム登録サーバは、さらに、加入者のディレクトリにアクセスすることで、詳細な加入者サービスプロフィル情報（例えば、加入するサービスオプションの品質等）を得る。ステップ７において、ホーム登録サーバがフォーリン登録サーバに、アクセス確認応答を送り返す。ステップ８において、フォーリン登録サーバがフォーリンエージェントにアクセス確認応答を転送する。ステップ９において、フォーリンエージェントがエンドシステム（つまり、モバイル）に登録確認応答を送り返す。

【００９７】以下では、ベアラデータを扱うプロトコルハンドリングのシナリオおよびベアラデータをエンドシステムとの間の送受するための関連するスタックを、ローカルAPを用いるセルアーキテクチャ（図１７）と、リモートAPを用いるセルアーキテクチャ（図１８）に対する両方のプロトコルスタックについて説明する。

【００９８】図１７は、ホームネットワーク内のエンドシステムとホームIWFとの間の通信を扱うためのプロトコルスタックをEnd System@Homeに対して示す。図１７は、アクセスポイントと無線ハブが同一位置に配置される場合のセルアーキテクチャに対するプロトコルハンドリングを示す。

【００９９】図１８は、アクセスポイントと無線ハブが離して配置される場合のセルアーキテクチャに対するプロトコルハンドリングを示す。図示するようにPPPはIWF内に終端し、この構成は直接インターネットアクセスを提供する。PPPサーバとIWFが離されるケースの構成については後に説明する。

【０１００】図１８に示すように、エンドシステムからのPPPフレームはRLP（radio link protocol）フレーム内にカプセル化され、これらはさらにリモートアクセスポイントの所でMACフレーム内にカプセル化され、トランクアクセスポイントに送信される。トランクアクセスポイントは、無線ハブと物理的に接近して位置するアクセスポイントであり、リモートアクセスポイントはトランクアクセスポイントに、一例として、無線トランクによって接続される。このリモートアクセスポイントは、MAC層ブリッジとして機能し、エアリンクからのフレームを無線ハブ内のフォーリンエージェントに中継する。フォーリンエージェントは、MACフレームからRLPフレームを取り出し、このRLPフレームをxtunnelプロトコルを用いてIWFに中継する。IWFからエンドシステムに送られるフレームの場合も方向が逆であることを除いて類似するプロセスが発生する。

【０１０１】エンドシステムが別のフォーリンエージェントに移動すると、新たなフォーリンエージェントとIWFとの間に新たなxtunnelが自動的に生成され、PPPトラヒックはこれらの間を中断されることなく運ばれる。

【０１０２】リモートAPとトランクAPとの間に無線トランクを用いるリモートAPセルアーキテクチャでは（図１８）、エンドシステムとアクセスポイントとの間のエアリンクは、トランクの無線技術および周波数（ｆ２）とは異なる無線技術および周波数（ｆ１）を用いて動作する。

【０１０３】図１９は、ローミングエンドシステムに対するプロトコルスタックを示す。サービングIWFは、サービングIWFとホームIWFとの間にI-xtunnelプロトコルを用いる。プロトコルスタックの他の部分は、上述と同一であるため特に示さない。

【０１０４】RLP層は、シーケンス番号を用いることで、重複するPPPデータグラムを脱落させ、エンドシステムとIWFとの間でPPPデータグラムをシーケンスに配信する。RLP層は、さらに、エンドシステムとIWFとの間のリンク接続性を監視するためにコンフィギャラブルキープアライブ機構を用いる。代替の実施例においては、RLP層は、さらに、エンドシステムとIWFとの間のリンクの総ビットエラー率を低減するために再送およびフロー制御サービスを提供する。エンドシステムとIWFの間のRLPはセッションの開始時に始動され、セッションを通じてハンドオフの間もアクティブにとどまる。

【０１０５】mobile IP RFC（RFC 2003）の仕様と対照的にフォーリンエージェントとホームエージェントとの間のトンネリングにIP in IP encapsulationは用いられない。この代わりに新たなトンネリングプロトコルがUDPの上に実現される。この新たなトンネリングプロトコルはL2TPプロトコルを簡素化したバージョンである。新たなこのトンネリングプロトコルを用いる理由は以下の通りである：

【０１０６】１．RFC 2003において規定されるカプセル化プロトコルでは、フロー制御、すなわちパケットのシーケンス配信は提供しない。ただし、本発明のネットワークはバックホールを通じてのトンネル内でこのサービスをエアリンクの上の再送の量を低減するために必要とする。つまり、フロー制御を用いることで、基地局とMSCとの間のネットワーク上のフロー制御問題に起因するパケット損失や、基地局あるいはIWF内のフロー制御問題に起因するパケット損失が低減される。

【０１０７】２．このトンネリングプロトコルはUDPベースであるため、ユーザレベルにて実現し、性能を保証するためのデバッグの後にカーネルに入れることができる。

【０１０８】３．RFC 2003を用いた場合、サービス品質と負荷バランスを考慮に入れてトンネリングを生成するのは簡単ではない。QOSを考慮に入れるためには、既に要求されるQOSを提供するリンク上にトンネルを設定できる必要がある。第二に、RFC2003を用いた場合は、基地局とMSCとの間の複数のリンクの間にベアラトラヒックを分散させ、負荷をバランスさせるのは簡単ではない。

【０１０９】４．RFC 2003において規定されるようにIP in IP encapsulationを実現するためには、開発者はIPソースコードへのアクセスが必要となる。商用のオペレーティングシステムの場合、TCP/IPスタックに対するソースコードは、通常、別個の商品（所有プログラム）として開発されており、他のベンダとの互換性がない。ベンダからTCP/IPスタックを購入し、mobile IP tunnelingをサポートするたにIP層に変更を加える場合、開発業者はTCP/IPスタックの様々なバージョンを絶えずサポートすることを要求される。これには追加のコストとリスクが伴う。

【０１１０】本発明による基地局とIWFとの間のトンネリングプロトコルは非標準であり、無線サービスプロバイダは異なるベンダからの装置を混合し、整合させることはできない。ただし、非標準のトンネリングプロトコルを単一の無線サービスプロバイダのネットワーク内で用いた場合、これは、エンドシステムや他のベンダからの装置には透過的であることに注意する。

【０１１１】この新たなトンネリングプロトコルはL2TPに基づく。L2TP自体は、重いトンネリングプロトコルであり、L2TPはトンネルの生成および認証と関連する大きなオーバーヘッドを持つ。L2TPと比べ、本発明による新たなトンネリングプロトコルはオーバヘッドが小さい。この新たなxtunnelプロトコルは、以下の特徴を持つ：

【０１１２】１．このxtunnelの生成は、基地局と登録サーバとの間で用いられるRadius Access Request（Radiusアクセス要求）と、Radius Access Response（Radiusアクセス応答）メッセージにベンダ固有の拡張を追加する。これら拡張はトンネルパラメータを協議し、トンネルを生成する。

【０１１３】２．登録サーバは、パケットをトンネリングおよび中継する実際の仕事は様々な異なるIPアドレス、従って、MSC内の異なるサーバに委託することができる。このため、登録サーバは、複数のIWFサーバ間で負荷のバランスを取ること、および様々なユーザに異なるQOSを提供することが可能になる。

【０１１４】３．このxtunnelプロトコルは、トンネル管理に対する帯域内制御メッセージをサポートする。これら制御メッセージとしては、トンネルの接続性をテストするためのエコーリクエスト／応答、トンネルを切断するための切断リクエスト／応答／通知、およびエラーを通知するためのエラー通知が含まれる。これらメッセージは、UDP/IP等のトンネリング媒体上を送信される。

【０１１５】４．このxtunnelプロトコルは、ペイロードデータをUDP/IP等のトンネリング媒体上に送信する。このxtunnelプロトコルは、フロー制御とパケットのシーケンス配信をサポートする。

５．このxtunnelプロトコルは、サービス品質を確保する目的でUDP/IP以外の媒体上に実現することもできる。

【０１１６】本発明によるネットワークは、直接インターネット接続性をサポートする。これは、PPP をホームIWF内に終端し、このIWFからのIPパケットをルータを介して標準のIPルーティング技術を用いてインターネットにルーティングすることで達成される。好ましくは、IWFとルータは両方ともRIPをランするが、場合によっては、OSPF等の他のルーティングプロトコルをランすることもできる。

【０１１７】このネットワークは、同時にインターネットサービスプロバイダでもある無線サービスプロバイダ（WSP）に対して第一の構成をサポートする。この構成においては、MSC内のホームIWFはPPPサーバとしても機能する。このホームIWFもRIP等のインターネットルーティングプロトコルをランし、インターネットサービスプロバイダのバックボーンネットワークへの接続するためにルータを用いる。

【０１１８】このネットワークは、WSP自身はインターネットサービスプロバイダ（ISP）ではないため、あるいはそのWSPがエンドユーザにアクセスを提供する合意を他のISPとの間でにもつために、エンドシステムを一つあるいは複数のインターネットサービスプロバイダに接続することを希望する無線サービスプロバイダに対して第二のコンフィギュレーションをサポートする。例えば、ある無線サービスプロバイダ（WSP）がエンドユーザにネットワークアクセスを提供することを選択し、さらに、第三者であるISPとの間に、その第三のISPとも取引のあるエンドユーザが、そのWSPネットワークからその第三のISPにアクセスするのを許す合意を持つ状況がこれに相当する。この構成においては、PPPサーバは、MSCの所に設置されるホームIWF内ではランしない。代わ

りに、L2TP（Layer Two Tunneling Protocol）等のトンネリングプロトコルを用いてISPのPPPサーバにトンネルバックする。図１０はこの構成に対するプロトコルスタックをホームに位置するエンドシステムに対して示す。

【０１１９】ホームIWFとISPのPPPサーバの位置は、PPPセッションを通じて固定されたままにとどまる。ホームIWFとISPのPPPサーバとの間のL2TPトンネルもPPPセッションを通じて設定されたままにとどまる。ホームIWFとPPPサーバとの間の物理リンクはルータを介して専用のT1もしくはT3、あるいはフレームリレーもしくはATMネットワークを用いて設定される。この物理リンクの個々の特性はこのアーキテクチャの観点からは特に重要ではない。

【０１２０】この構成は、イントラネットアクセスもサポートする。イントラネットアクセスの場合は、PPPサーバは企業イントラネット内に駐在し、ホームIWFはL2TPを用いてこれにトンネリングする。

【０１２１】図２０は、イントラネットあるいはISPアクセスに対するプロトコルハンドリングをローミングエンドシステムに対して示す。これは、上述の構成とは、ローミングエンドシステムがサービングIWFを用いて自身のホームIWFに接続する点が異なる。サービングIWFとホームIWFとの間のプロトコルハンドリングは前述の通りである。

【０１２２】図２１は、登録フェーズ、つまり、エンドシステムの登録の際に用いられるプロトコルスタックをローカルAPセルアーキテクチャに対して示す。リモートAPセルアーキテクチャに対するプロトコルスタックもこれとほぼ同一である。上述のシナリオはローミングエンドシステムに対するものであり、ホームに位置するエンドシステムに対しては登録経路内にはフォーリン登録サーバは関与しない。

【０１２３】エンドシステム内のモビィリティエージェントについても説明の必要がある。エンドシステム内のモビィリティエージェントと無線ハブ内のフォーリンエージェントは、概念的に、mobile IP RFC 2002と類似する。このモビィリティエージェントは、ネットワークエラーをタイムアウトと再試行を用いて扱う。ベアラデータに対する周知のプロトコルスタックと異なり、RLP層は用いられない。フォーリンエージェントと登録サーバはエンドシステムの登録のためにRadius overUDP/IPを用いて互いに通信する。

【０１２４】セキュリティに関して幾つかの点を説明する必要がある。第一に、エンドシステムの識別とフォーリン／ホームネットワークの識別が、無線登録フェーズの際に認証（検証）される。第二に、エンドシステムの識別が自身のPPPサーバに対してPPP認証フェーズの際に認証（比較）される。第三に、アカウンティングデータの格納、課金、およびホームドメイン情報の更新の際に認証が行なわれる。第四に、エンドシステムとの間で送受されるベアラトラヒックは暗号化される。第五に、サービスプロバイダの境界を越えて課金情報を交換する際は暗号化が行なわれる。

【０１２５】無線登録の際のエンドシステムの識別のそれらのホームネットワークに対する認証（比較）およびホームネットワークとフォーリンネットワークの識別の認証には、共有のセキュリティが用いられる。

【０１２６】エンドシステムの認証においては、１２８ビットの共有のセキュリティを用いてその登録リクエストに対する認証子が生成される。この認証子は、mobile IPRFC 2002において指定される周知のMD５メッセージダイジェストアルゴリズムを用いて生成される。エンドシステムは、この共有のセキュリティを登録リクエストに入れて送信することはなく、認証子のみを送信する。エンドシステムから登録リクエストを受信すると、ホーム登録サーバは、登録リクエストデータから共有のセキュリティを用いて認証子を再計算する。再計算した認証子の値がエンドシステムによって送信された認証子の値と一致する場合は、ホーム登録サーバは、以降の登録プロセスの進行を許可する。両方の値が一致しない場合は、ホーム登録サーバは、この事象を登録し、セキュリティ違反警告およびこのリクエストに対する否定通知（nak）を生成する。

【０１２７】登録応答を送り返すとき、ホーム登録サーバは上述と同一の手続きを遂行する。つまり、共有のセキュリティを用いて登録応答に対する認証子を生成し、これをエンドシステムに送信する。登録応答を受信すると、エンドシステムは共有のセキュリティを用いて認証子を再計算する。再計算した値がホーム登録サーバによって登録応答に入れて送られた認証子の値と一致しない場合は、エンドシステムは、その応答を破棄し、再び認証を試みる。

【０１２８】これらのネットワークセキュリティ概念は、mobile IP RFC 2002において定義されている概念と類似する。RFCによると、各エンドシステムとそのホームネットワークとの間には、モビィリティセキュリティアソシエーションが存在する。各モビィリティセキュリティアソシエーションは、セキュリティ文脈のコレクションを定義する。各セキュリティ文脈は、認証アルゴリズム、モード、セキュリティ（共有、公開、プライベート）、応答保護のスタイル、および用いる暗号化のタイプを定義する。本発明の背景においては、エンドシステムのUser-Nameが（ホームアドレスの代わりに）、各エンドシステムとそのホームネットワークとの間のモビィリティセキュリティアソシエーションを識別するために用いられる。セキュリティパラメータインデックス（SPI）と呼ばれるもう一つのパラメータがモビィリティセキュリティアソシエーション内の特定のセキュリティ文脈を選択するために用いられる。本発明の基本的な実施例においては、デフォルトmobile IP authenticationア

ルゴリズム（keyed-MD5）およびデフォルトモード（“prefix+suffix”）のみが１２８ビットの共有のセキュリティにてサポートされる。ネットワークユーザは、自身のホームネットワークとの間で複数の共有のセキュリティを定義することが許される。エンドユーザに対するセキュリティ文脈の生成、セキュリティパラメータインデックス（SPI）の各セキュリティ文脈への割り当て、セキュリティ文脈の内容（共有のセキュリティを含む）の設定、内容の修正等を遂行するための機構については後に説明する。登録の際に、エンドシステムは、１２８－ビットのメッセージダイジェストを、接頭語＋接尾語モードにて、MD5アルゴリズムを用いて計算する。このとき、共有のセキュリティを登録リクエスト内の保護されるべきデータに対する接頭語および接尾語として用いる。次に、エンドシステムは、こうして計算した認証子を、SPIおよびUser-Nameと一緒に、登録リクエストに入れて送信する。エンドシステムの登録リクエストを受信すると、フォーリン登録サーバは、このリクエストを、認証子およびSPIと一緒に、変更を加えずに、ホーム登録サーバに中継する。エンドシステムから直接あるいはフォーリン登録サーバを介して間接的に登録リクエストを受信すると、ホーム登録サーバは、そのSPIおよびUser-Nameを用いてセキュリティ文脈を選択する。次に、ホームサーバは共有のセキュリティを用いて認証子を再計算する。再計算した認証子の値がエンドシステムによって登録リクエストに入れて送られた認証子の値と一致する場合は、ユーザの識別の認証は成功する。一致しない場合は、ホーム登録サーバは、エンドシステムによって送信された登録リクエストに対して否定の応答を送り返す。

【０１２９】ホーム登録サーバによってエンドシステムに送られる登録応答も上述のmobileIPアルゴリズムを用いて認証（検証）される。ホームサーバは、SPIおよび計算した認証子の値を登録応答メッセージに入れてエンドシステムに送信する。登録応答を受信すると、エンドシステムは認証子を再計算し、再計算した値が送信した値と一致しない場合は、その登録応答を破棄し、再び認証を試みる。

【０１３０】ユーザのエンドシステムは、共有のセキュリティおよびユーザが自身の登録サーバと共有する全てのセキュリティ文脈に対するSPIを持つように構成する必要がある。このコンフィギュレーション情報は、好ましくは、Windows 95ベースのエンドシステムの場合は、Win 95レジストリに格納する。登録の際に、この情報がアクセスされ、認証の目的で用いられる。

【０１３１】ネットワーク内において、フォーリンエージェント（FA）は、エンドシステムに代わってエンドシステムの登録を行なうため、および無線ハブとホームIWFあるいはサービングIWFの間のxtunnelを構成するためにRadiusプロトコルを用いる。エンドシステムから登録リクエストを受信すると、FAは、Radius Access-Requestパケットを生成し、このパケット内に自身の属性を挿入し、さらに、エンドシステムの登録リクエストの属性を、変更を加えずに、このパケット内にコピーし、こうして結合したリクエストをMSC内の登録サーバに送信する。

【０１３２】Radius認証には、Radiusクライアント（この場合は基地局内のＦＡ）とRadiusサーバ（この場合はMSC内の登録サーバ）が、認証のためにセキュリティを共有することが必要とされる。この共有のセキュリティは、RadiusクライアントとRadiusサーバの間で通信されるプイラベート情報の暗号化にも用いられる。この共有のセキュリティは、コンフィガラブルなパラメータである。ネットワークは、Radius RFCの勧告に従って共有のセキュリティおよびMD5アルゴリズムを認証のために用い、暗号化が必要とされる場合は、暗号化のためにも用いる。FAによって送信されるRadius Access-Requestパケットは、Radius User-Name属性（これはエンドシステムによって供給される）およびRadius User-Password属性を含む。User-Password属性の値もコンフィガラブルな値であり、Radiusプロトコルによって勧告される方法に従って暗号化される。Radius RFC標準の観点からは非標準属性であるネットワークに特定な他の属性も、ベンダ固有のRadius属性として符号化され、Access-Requestパケットに入れて送信される。

【０１３３】FAは以下の属性をRadius Access-Requestパケットに挿入して登録サーバに送信する：

１．User-Name Attribute（ユーザ名属性）。これはエンドシステムのユーザ名であり、エンドシステムによって登録リクエストに入れて供給される。

２．User-Password Attribute（ユーザパスワード属性）。このユーザパスワードは、基地局／無線ハブによってユーザに代わって供給される。これは、Radius EFCの規定に従って基地局とその登録サーバとの間で共有されるセキュリティを用いて符号化される。

【０１３４】３．NAS-Port（NASポート）。これは基地局上のポートである。

４．NAS-IP Address（NAS-IPアドレス）。これは基地局のIPアドレスである。

５．Service-Type（サービスタイプ）。これはフレームドサービスである。

【０１３５】６．Framed Protocol（フレームドプロトコル）。これはPPPプロトコルである。

７．Xtunnel Protocol Parameters（Xtunnelプロトコルパラメータ）。これらのパラメータは基地局によってエンドシステムに代わってxtunnelプロトコルを設定するための必要なパラメータを指定するために送信される。これはベンダ固有の属性である。

【０１３６】８．AP-IP Address（AP-IP アドレス）。これはユーザが登録の際に用いるAPのIPアドレスであ

る。これはベンダ固有の属性である。
９．AP-MAC-Address（AP-MACアドレス）。これはユーザが登録の際に用いるAPのMACアドレスである。
１０．End system's Registration Request（エンドシステムの登録リクエスト）。エンドシステムからの登録リクエストは、変更を加えず、このベンダ固有の属性内にコピーされる。
【０１３７】登録サーバは以下の属性をRadius Access-Responseパケットに入れてFAに送り返す：
１．Service Type（サービスタイプ）。これはフレームドサービスである。
２．Framed-Protocol（フレームドプロトコル）。これはPPPである。
３．Xtunnel Protocol Parameters（Xtunnelプロトコルパラメータ）。これらのパラメータは登録サーバによってエンドシステムに代わってxtunnelプロトコルを設定するために必要なパラメータを指定するために送られる。これはベンダ固有の属性である。
【０１３８】４．Home Resistration Server'Replay（ホーム登録サーバの応答）。この属性は、ホーム登録サーバからFAに送信される。FAは、この属性を、変更を加えずに、登録応答パケットに入れてエンドシステムに中継する。経路内にフォーリン登録サーバが存在する場合は、フォーリン登録サーバは、この属性を、変更を加えずに、FAに中継される。これはベンダ固有の属性として符号化される。
【０１３９】ローミングエンドシステムにサービスを提供するためには、フォーリンネットワークとホームネットワークが互いにアカウンティングおよび課金の目的で、認証とコンフィギュレーションのためにRadiusプロトコルを用いて認証（検証）される。この認証はエンドシステムが登録するときに遂行される。上述のように、フォーリンネットワーク内の登録サーバは、エンドシステムからの登録リクエスト（これはFAによってRadius-Access Requestパケット内にベンダ固有の属性としてカプセル化して中継される）を受信すると、このフォーリン登録サーバは、エンドシステムのNser-Nameを用いて、自身のホームドメインディレクトリ（HDD）を調べることで、エンドシステムのホーム登録サーバの識別を見つける。ホームドメインディレクトリ（HDD）には、以下の情報が格納されており、フォーリン登録サーバはエンドシステムの登録リクエストを転送するためにこれにアクセスする：
【０１４０】１．Home Registration Server IP Address（ホーム登録サーバのIPアドレス）。これは登録リクエストの転送先のホーム登録サーバのIPアドレスである。
【０１４１】２．Foreign Registration Server Machine Id（フォーリン登録サーバのマシンId）。これは、フォーリン登録サーバのSMTP（simplified mail transfer prorocol）フォーマットでのマシンIDである（これは、例えば、machine@fqdnの形式を持ち、マシン（machine）はフォーリン登録サーバマシンの名前を表し、fqdnはフォーリン登録サーバのドメインの完全修飾ドメイン名である）。
【０１４２】３．Tunneling Protocol Parameters（トンネリングプロトコルパラメータ）。これらは、エンドシステムに代わってサービングIWFとホームIWFとの間のトンネルを構成するためのパラメータである。これらパラメータには、これらの間で用いられるべきトンネリングプロトコルとトンネルを構成するためのパラメータが含まれる。
【０１４３】４．Shared Secret（共有のセキュリティ）。これはフォーリン登録サーバとホーム登録サーバとの間の認証のために用いられるべき共有のセキュリティである。このセキュリティは、フォーリン登録サーバからホーム登録サーバに送信されるRadius User-Password属性を計算するために用いられる。これは、２つの無線サーバプロバイダの間で定義される。
【０１４４】５．User-Password（ユーザパスワード）。これはローミングエンドシステムに代わって用いられるべきユーザパスワードである。このユーザパスワードは、２つの無線サービスプロバイダの間で定義される。このパスワードはRadius RFCの規定に従って共有のセキュリティを用いて暗号化される。
【０１４５】６．Accounting Parameters（アカウンティングパラメータ）。これらは登録するエンドシステムに代わって、アカウンティングを構成するためのパラメータである。これらパラメータは、登録サーバによって自身のIWFにエンドシステムに代わってアカウンティングを構成するために送信される。
【０１４６】フォーリン登録サーバは、上述の情報を用いてRadius Access-Requestを生成し、このRadius Access-Requestに自身の登録および認証情報を追加し、さらにこのRadius Access-Request内にエンドシステムから送信された登録情報を、変更を加えずに、コピーし、こうして結合したリクエストをホーム登録サーバに送信する。
【０１４７】ホーム登録サーバは、Radius-Access Requestをエンドシステムがローミングしている場合はフォーリン登録サーバを介して受信し、エンドシステムがホームに位置する場合はFAから直接に受信するが、これを受信すると、後者の場合は自身のディレクトリサーバに照会して共有のセキュリティを得ることでエンドシステムの検証を行なう。一方、エンドシステムがローミングしている場合は、フォーリン登録サーバの識別を認証子を再計算することで検証する。
【０１４８】リクエストの認証に成功した場合は、ホーム登録サーバは、Radius Access-Accept応答パケットを生成し、これをエンドシステムがローミングしている場

合はフォーリン登録サーバに送り返す。一方、エンドシステムがホームに位置する場合は、これをRadius-Access Requestを送信してきたFAに直接に送り返す。この応答には、登録応答属性が含まれ、FAは、これをエンドシステムに中継する。

【０１４９】他方、リクエストの認証に失敗した場合は、ホーム登録サーバは、Radius Access-Reject応答パケットを生成し、これを、エンドシステムがローミングしている場合はフォーリン登録サーバに返信する。一方、エンドシステムがホームに位置する場合は、Radius-Access Requestを送信してきたFAに直接に送り返す。この応答には、登録応答属性が含まれ、FAは、これをエンドシステムに中継する。

【０１５０】エンドシステムがローミングしているシナリオにおいては、ホーム登録サーバからの応答はフォーリン登録サーバによって受信され、これはフォーリン登録サーバによって共有のセキュリティを用いて認証（検証）される。認証の後に、フォーリン登録サーバは、応答を処理することで、自身のFAに送信するためのRadius応答パケット（AccessあるいはReject）を生成する。このとき、フォーリン登録サーバは、ホーム登録サーバによって返信されたRadius応答パケットからの登録応答属性を、変更を加えることなく、FAに送信するRadius応答パケット内にコピーする。

【０１５１】FAは、Radius Access-ResponseあるいはRadius Access-Reject応答パケットを受信すると、このRadius応答からの登録応答属性を用いて、登録応答パケットを生成し、この応答パケットをエンドシステムに送信する。これによってラウンドトリップ登録シーケンスが完了する。

【０１５２】Mobile IP標準は、登録応答の保護を、タイムスタンプを用いて、あるいはオプションしてノンス（nonces）を用いて実現することを指定する。ただし、タイムスタンプを用いての応答の保護には、対応するノード間に正確に同期された日時クロックが要求される。このため、Mobile IP標準ではタイムスタンプの使用が強制でノンスの使用はオプションであるが、本発明では、登録の際の応答の保護はノンスを用いて実現される。ただし、代替として、タイムスタンプを用いて応答の保護を実現することも考えられる。

【０１５３】ノード間で用いられる応答保護のスタイルは、セキュリティ文脈内に認証文脈、モード、セキュリティ、暗号化のタイプと一緒に格納される。ネットワークはエンドシステムとそのPPPサーバとの間のPPPベースでのPAP（パスワード認証）およびCHAP（パスワード認証の挑戦）の使用をサポートする。これは、前述のmobile IPおよびRadiusベースの認証機構とは独立に行なわれる。これは、プライベートイントラネットあるいはISPがユーザの識別を独立に検証することを可能にする。

【０１５４】以下では、アカウンティングおよびディレクトリサービスに対する認証を、アカウンティングセキュリティとの関連で説明する。同一MSC内のネットワーク装置からのディレクトリサーバへのアクセスの場合、認証は必要とされない。

【０１５５】ネットワークは、エンドシステムとホームIWFとの間で伝送されるベアラデータの暗号化をサポートする。エンドシステムは、該当するセキュリティ文脈を選択することで、暗号化がオンあるいはオフされることを指定する（協議する）。登録リクエストが受信されたとき、ホーム登録サーバは、エンドシステムの暗号化に対するリクエストをセキュリティ文脈に基づいて許可する。認証アルゴリズム、モード、共有のセキュリティ、および応答保護のスタイルを格納するのに加えて、セキュリティ文脈が用いるべき暗号化アルゴリズムのスタイルを指定するためにも用いられる。エンドシステムとホームエージェントとの間の暗号化が協議（指定）されている場合は、PPPフレーム全体を指定通りに暗号化した後に、これをRLPにカプセル化する。

【０１５６】IWF、アカウンティングサーバ、およびアカウンティングシステムは、MSC内の同一の信託されたドメイン（trusted domain）の一部分である。これらエンティティは、同一LAN上に接続されるか、あるいは無線サービスプロバイダによって所有および運用される信託されたイントラネットの一部分に接続される。IWFとアカウンティングサーバとの間、並びにアカウンティングサーバと顧客の課金システムとの間のアカウンティング統計の転送は、暗号化する必要はない。

【０１５７】このネットワークでは、エンドシステムの位置をモニタすることは、より困難になる。これは、エンドシステムとの間で伝送される全てのPPPフレームが、エンドシステムデバイスの実際の位置と関係なく、ホームIWFを通過するように見えるためである。

【０１５８】アカウンティングデータは、ネットワーク内のサービングIWFとホームIWFによって集められる。サービングIWFによって集められたアカウンティングデータは、サービングIWFのMSC内のアカウンティングサーバに送られる。ホームIWFによって集められたアカウンティングデータは、ホームIWFのMSC内のアカウンティングサーバに送られる。サービングIWFによって集められたアカウンティングデータは、フォーリン無線サービスプロバイダによって、監査のため、および請求書を無線サービスプロバイダの境界間で清算するために用いられる（これによって、ローミングとモビィリティがサポートされる）。ホームIWFによって集められたアカウンティングデータは、エンドユーザに対する請求書を作成するために、および請求書を無線サービスプロバイダの境界間で、ローミングとモビィリティをサポートするために清算するために用いられる。

【０１５９】全てのデータトラヒックが、エンドシステムの位置およびフォーリンエージェントの位置に関係な

く、ホームIWFに送られるために、ホームIWFは、顧客の請求書を生成するため、および、フォーリンネットワークの使用に関する清算情報を生成するための全ての情報を持つ。

【０１６０】サービングIWFおよびホームIWFは、登録したエンドシステムに対するアカウンティングレコードを送信するために、好ましくは、Radiusアカウンティングプロトコルを用いる。Radiusアカウンティングプロトコルは、ドラフトIETF RFCにおいて規定される通りである。本発明では、このプロトコルが拡張される。つまり、このRadius Accountingプロトコルに、このネットワークに対するベンダ固有の属性と、チェックポインティングが追加される。チェックポインティングとは、この背景においてはアカウンティングデータの定期的な更新を意味し、これによってアカウンティングレコードが失われる危険性を最小に押さえられる。

【０１６１】RadiusアカウンティングプロトコルはUDP/IP上でランし、確認応答（アクノレッジメント）とタイムアウトに基づく再試行を用いる。Radiusアカウンティングクライアント（サービングIWFあるいはホームIWF）は、UDPアカウンティングリクエストパケットを自身のアカウンティングサーバに送信する。すると、アカウンティングサーバは、アカウンティングクライアントに確認応答を送り返す。

【０１６２】ネットワーク内において、アカウンティングクライアント（サービングIWFおよびホームIWF）は、ユーザセッションが開始されるとアカウンティング開始指標を送信し、ユーザセッションが終了するとアカウンティング停止指標を送信する。アカウンティングクライアントは、さらに、セッション最中にもアカウンティングチェックポイント指標を送信する。これとは対照的に、IETF RFCドラフトRadiusアカウンティングは、アカウンティングチェックポイント指標は指定しない。本発明のソフトウエアは、この目的のためにベンダ固有のアカウンティング属性を生成する。このアカウンティング属性は、Acct-Status-Type of Start（アカウンティング開始指標）を含む全てのRadius Accounting-Requestパケット内に存在する。この属性の値は、アカウンティングサーバに、そのアカウンティングレコードがチェックポインティングレコードであるか否かを通知するために用いられる。チェックポインティングアカウンティングレポートは、時間属性を持ち、セッションが開始されてからの累積アカウンティングデータを含む。本発明においては、チェックポインティングパケットの送信頻度はコンフィガラブルである。

【０１６３】サービングIWFおよびホームIWFは、各自の登録サーバによって、登録フェーズの際に、各自のアカウンティングサーバに接続されるように構成される。コンフィガラブルアカウンティングパラメータには、アカウンティングサーバのIPアドレスおよびUDPポート、チェックポインティングの頻度、セッション／マルチセッションのID、およびアカウンティングクライアントとアカウンティングサーバとの間で用いられるべき共有のセキュリティが含まれる。

【０１６４】ネットワークは、各登録したエンドシステムに対して、以下のアカウンティング属性を記録する。これらアカウンティング属性は、セッションの開始時、セッションの終了時、および中間（チェックポイント）において、アカウンティングクライアントによって、それらのアカウンティングサーバに、Radiusアカウンティングパケットに入れて報告される。このRadiusアカウンティングパケットは、以下を含む：

【０１６５】１．User Name（ユーザ名）。これは上述のRadius User-Name属性と類似する。この属性はユーザを識別するために用いられ、全てのアカウンティングレポート内に存在する。フォーマットは“user@domain”の形式を持ち、ドメインは（domain）は、ユーザのホームの完全修飾ドメイン名を表す。

【０１６６】２．NAS IP Address（NAS IP アドレス）。これは上述のNAS-IP-Address属性と類似する。この属性は、ホームIWFあるいはサービングIWFをランしているマシンのIPアドレスを識別するために用いられる。

３．Radio Port（無線ポート）。この属性はユーザにサービスを提供するアクセスポイント上の無線ポートを識別する。この属性はベンダ固有の属性として符号化される。

【０１６７】４．Access Point IP Address（アクセスポイントIPアドレス）。この属性はユーザにサービスを提供しているアクセスポイントのIPアドレスを識別する。この属性はベンダ固有の属性として符号化される。

５．Service Type（サービスタイプ）。これは上述のRadius Service-Type属性と類似する。この属性の値はFramedである。

６．Framed Protocol（フレームドプロトコル）。これは上述のRadius Framed-Protocol属性と類似する。この属性の値はPPPを示すように設定される。

【０１６８】７．Accounting Status Type（アカウンティング状態のタイプ）。これは上述のRadius Acct-Status-Type属性と類似する。この属性の値は、ユーザのRadiusクライアントとのセッションの開始を示すStart（開始）か、ユーザのRadiusクライアントとのセッションの停止を示すStop（停止）である。アカウンティングクライアントに対しては、Acct-Status-Type/Start属性はエンドシステムが登録したときに生成され、Acct-Status-type/Stop属性はエンドシステムがなんらかの理由で登録を解除したときに生成される。チェックポイントに対しては、この属性の値はStartであり、Accounting Checkpoint（アカウンティングチェックポイント）属性も存在する。

【０１６９】８．Acounting Session ID（アカウンティ

ングセッションのID）。これは上述のRadius-Session-Idと類似する。エンドシステムがローミングしているシナリオでは、このセッションIDは、エンドシステムが登録リクエストを発行したときにフォーリン登録サーバによって割り当てられる。これは登録シーケンスの際にフォーリン登録サーバからホーム登録サーバに送信される。ホームネットワークとフォーリンネットワークの両方ともAcct-Session-ID属性を知っており、この属性を各自のアカウンティングサーバにアカウンティングレコードを送信する際に送信する。“エンドシステムがホームに存在する”シナリオでは、この属性はホーム登録サーバによって生成される。ホーム登録サーバは、この属性の値を、自身のIWFに通知する。すると、IWFはこれを全てのアカウンティングレコード内に挿入する。

【０１７０】９．Accounting Multi-Session ID（アカウンティングマルチセッションのID）。これは上述のRadius Acct-Multi-Session-IDと類似する。このIDは、ホーム登録サーバによって、エンドシステムに代わって登録リクエストがFAから直接に受信されたとき、あるいはこれがフォーリン登録サーバを介して受信されたときに割り当てられる。これはホーム登録サーバからフォーリン登録サーバに登録応答メッセージに挿入して送られる。フォーリン登録サーバは、この属性の値を、自身のIWFに送り、IWFはこれを全てのアカウンティングレコードに挿入する。

【０１７１】本発明ではアーキテクチャに真のモビィリティが追加されるが、このIDは、エンドシステムが、あるIWFから別のIWFに移動した場合に、同一のエンドシステムに対する異なるIWFからのアカウンティングレコードを一つに纏めるために用いられる。IWF境界間でハンドオフした場合、IWFが変わるとアカウンティングレコード内のAcct-Session-Idも変わる。ただし、Acct-Multi-Session-Idの属性は、そのユーザにサービスを提供した全てのIWFが、アカウンティングレコード内に同一の値を用いる。セッションIDとマルチセッションIDは、フォーリンネットワークとホームネットワークの両方によって知られていおり、両ネットワークはこれらの属性をアカウンティングレポートに挿入し、各自のアカウンティングサーバに送る。課金システムはこれらセッションIDおよびマルチセッションIDを用いて同一無線サービスプロバイダのIWF境界間あるいは異なる無線サービスプロバイダの境界間からのアカウンティングレコードを一つに纏める。アカウンティングレコードには以下が含まれる：

【０１７２】１．Accounting Delay Time（アカウンティング遅延時間）。Radius Acct-Delay-Timeの属性を参照されたい。

２．Accounting Input Octets（アカウンティング入力オクテット）。RadiusAcct-Input-Octetsを参照されたい。この属性はエンドシステムから送信される（エンドシステムからネットワークに入力される）オクテットの数を追跡するために用いられる。このカウントは、もっぱらPPPフレームを追跡するために用いられ、エアリンクのオーバーヘッドや、RLPその他によって生じるオーバヘッドはカンウトされない。

【０１７３】３．Accounting Output Octets（アカウンティング出力オクテット）。RadiusAcct-Output Octetsを参照されたい。この属性はエンドシステムに送られる（ネットワークからエンドシステムに出力される）オクテットの数を追跡するために用いられる。このカウントはもっぱらPPPフレームを追跡するために用いられ、エアリンクのオーバーヘッドや、RLPその他によって生じるオーバヘッドはカンウトされない。

【０１７４】４．Accounting Authentic（アカウンティング認証）。Radius Acct-Authenticの属性を参照されたい。この属性の値はそのアカウンティングレコードがサービングIWFによって生成されたかホームIWFによって生成されたかにによってLocal（ホーム）かRemote（フォーリン）のいずれかを取る。

【０１７５】５．Accounting Session Time（アカウンティングセッション時間）。RadiusAcct-Session Timeの属性を参照されたい。この属性はユーザがサービスを受けた時間の量を示す。サービングIWFによって送信された場合は、この属性はユーザがそのサービングIWFからサービスを受けた時間の量を追跡する。ホームIWFによって送信された場合は、この属性はユーザがそのホームIWFからサービスを受けた時間の量を追跡する。

【０１７６】６．Accounting Input Packets（アカウンティング入力パケット）。Radius Acct-Input Packetsの属性を参照されたい。この属性はエンドシステムから受信されたパケットの数を追跡する。サービングIWFの場合は、この属性はエンドシステムからそのサービングIWFに入力されたPPPフレームの数を追跡する。ホームIWFの場合は、この属性はエンドシステムからそのホームIWFに入力されたPPPフレームの数を追跡する。

【０１７７】７．Accounting Output Packets（アカウンティング出力パケット）。RadiusAcct-Output Packetsの属性を参照されたい。この属性はエンドシステムに送信されたパケットの数を示す。サービングIWFの場合は、そのサービングIWFからエンドシステムに送信されたPPPフレームの数を追跡する。ホームIWFの場合は、この属性はそのホームIWFからエンドシステムに送信されたPPPフレームの数を追跡する。

【０１７８】８．Accounting Terminate Cause（アカウンティング終端原因）。Radius Acct-Causeの属性を参照されたい。この属性はユーザセッションが終端された理由を示す。加えて、追加の詳細を与えるために特定の原因コードも存在する。この属性はセッション終端時のアカウンティングレポート内にのみ存在する。

【０１７９】９．Network Accounting Terminate Cause

（ネットワークアカウンティング終端原因）。この属性はセッションが終端された詳細な理由を示す。この特定属性はベンダ固有の属性として符号化され、セッション終端時のみにRadius Accounting属性内に挿入して報告される。標準Radius属性であるAcct-Terminate Causeも存在する。この属性はAcct-Terminate Cause属性によってはカバーされない特定な原因コードを提供する。

【０１８０】１０．Network Air link Access Protocol（ネットワーク空中リクンアクセスプロトコル）。この属性はエンドシステムによって用いられるエアリンクアクセスプロトコルを示す。この属性はベンダ固有の属性として符号化される。

【０１８１】１１．Network Backhaul Access Protocol（ネットワークバックホールアクセスプロトコル）。この属性はアクセスポイントとエンドシステムとの間でデータを送受するために用いられるバックホールアクセスプロトコルを示す。この属性はベンダ固有の属性として符号化される。

【０１８２】１２．Network Agent Machine Name（ネットワークエージェントマシン名）。これはホームIWFあるいはサービングIWFをランするマシンの完全修飾ドメイン名である。この特定属性はベンダ固有の属性として符号化される。

【０１８３】１３．Network Accounting Check-point（ネットワークアカウンティングチェックポイント）。RFCドラフトRadiusアカウンティングは、チェックポイントパケットは定義しないために、本発明によるネットワークは、Radiusアカウンティング開始パケット内にこの属性を用いることでチェックポイントをマークする。このチェックポイント属性の存在しない場合は、従来のアカウンティング開始パケットであることを意味する。アカウンティング開始パケット内にこの属性が存在する場合は、それがアカウンティングチェックポイントパケットであることを意味する。アカウンティング停止パケットの場合はこの属性は含まない。

【０１８４】好ましい実施例においては、全てのアカウンティングパケットおよび対応する確認応答は、MD5および共有のセキュリティを用いて認証（検証）されることを必要とする。IWFは共有のセキュリティを備えるように構成され、IWFは自身のRaiusアカウンティングサーバと通信する際に、この共有のセキュリティを認証のために用いる。IWFによってアカウンティングサーバと通信するために用いられる共有のセキュリティは、MSC内に位置するホーム／フォーリンドメインディレクトリ内に格納される。アカウンティングセキュリティのために用いられるこれら共有のセキュリティは、エンドシステムの登録シーケンスの際に、登録サーバからIWFに送られる。

【０１８５】アカウンティングサーバソフトウエアはMSC内に位置するコンピュータ内でランする。システム内でのアカウンティングサーバの役割は、ネットワーク要素（ホームIWFおよびサービングIWF）から生のアカウンティングデータを集め、このデータを処理および格納し、その後、これを無線サービスプロバイダの課金システムに転送することにある。アカウンティングサーバは、課金システムは含まず、これは、自動あるいは手動のアカウンティングデータ転送機構をサポートする。自動のアカウンティングデータ転送機能を用いる場合は、アカウンティングサーバは、アカウンティングレコードを、AMA課金フォーマットにて、顧客の課金システムにTCP/IPトランスポート層を通じて転送する。この目的のために、システムはパケットデータに対するAMA課金レコードフォーマットを定義する。手動の転送機構を用いる場合は、顧客は、アカウンティングレコードを課金システムに転送するためのテープを構築する。顧客の仕様に合わせてテープが構築できるように、顧客にはアカウンティングレコードにアクセスするための情報が提供される。顧客はこの情報を用いてアカウンティングレコードを処理し、これをテープに書き込む。

【０１８６】図２２は、ホームIWFあるいはサービングIWFからアカウンティングサーバによって受信された生のアカウンティングデータが、アカウンティングサーバによって処理および格納される様子を示す。アカウンティングサーバによって遂行される処理には、IWFから受信された生のアカウンティングデータのフィルタリング、圧縮、および相関が含まれる。現用／待機二重のプロセッサと、ホットスワップが可能な高速ディスクとを用いる高アビイラビィリティのファイルサーバが、アカウンティングデータをアカウンティングサーバに送信する際に、データを一時的に緩衝するために用いられる。

【０１８７】アカウンティングサーバは、生のアカウンティングデータの処理を、エンドシステムがそのmobile IPセッションを終了するまで遅延させる。エンドシステムがセッションを終了すると、アカウンティングサーバはそのセッションを通じて集められた生のアカウンティングデータを処理し、アカウンティングサマリ（要約）レコードを、SQLデータベースに格納する。SQLデータベースに格納されるアカウンティングサマリレコードは、ASN.1符号化されたファイル（ASN.1 encodedfile）をポイントする。このファイルは、エンドシステムのセッションに関する詳細なアカウンティング情報を含む。アカウンティングサーバ内に格納されたデータは、次に、課金データ転送エージェントによって顧客の課金システムに転送される。別の方法として、無線サービスプロバイダがアカウンティングデータをSQLデータベースおよび／あるいはASN.1符号化されたファイルからテープを介して課金システムに転送することもできる。データベーススキームとASN.1符号化されたファイルのフォーマットが、顧客がこれを利用できるようにドキュメント化され、顧客に供給される。アカウンティングシステ

ム内に格納されている処理済みのアカウンティングデータの量が高水位マークを超えると、アカウンティングサーバはNMS警告を発行する。この警告はアカウンティングサーバ内に格納されているデータの量が低水位マーク以下に落ちると解除される。警告を発する高水位マークおよび警告を解除する低水位マークは、コンフィガラブルである。アカウンティングサーバは格納されているアカウンティングデータの年令があるコンフィガラブルな閾値を超えた場合も、NMS警告を発行する。逆に、この警告はアカウンティングデータの年令がこの閾値以下に落ちたときは解除される。

【０１８８】加入者ディレクトリは、加入者に関する情報を格納するために用いられ、ホームネットワーク内に設置される。ホーム登録サーバは、登録フェーズの際に、エンドシステムの認証および登録のために、このディレクトリを調べる。各加入者に対して、加入者ディレクトリは、以下の情報を格納する：

【０１８９】１．User-Name（ユーザ名）。加入者レコード内のこの欄は、SMTPフォーマット（例えば、user@fqdn）の形式を持ち、userサブ欄は、加入者を加入者の無線ホームドメインにて識別し、fqdnサブ欄は、加入者の無線ホームドメインを識別する。この欄は、エンドシステムによって登録フェーズの際に登録リクエストに挿入して送信される。この欄は、無線サービスプロバイダによって加入者にネットワークサービスに加入するときに割り当てられる。この欄はPPPにおいて用いられるユーザ名欄とは異なる。

【０１９０】２．Mobility Security Association（モビィリティセキュリティアソシエーション）。加入者レコード内のこの欄は、加入者とそのホームネットワークとの間のモビィリティセキュリティアソシエーションを含む。上述のように、各加入者とそのホーム登録サーバとの間には、モビィリティセキュリティアソシエーションが存在する。このモビィリティセキュリティアソシエーションは、セキュリティ文脈のコレクションを定義し、各セキュリティ文脈は、認証アルゴリズム、認証モード、共有のセキュリティ、応答保護のスタイル、およびエンドシステムとホームサーバとの間で用いるべき暗号化のタイプ（無暗号化も含む）を含む。登録の際、ホーム登録サーバは、エンドシステムによって登録リクエストに挿入して供給されるUser-Nameおよびsecurity parameter index（SPI）を用いてこの加入者ディレクトリからその加入者のセキュリティ文脈に関する情報を取り出す。このセキュリティ文脈内の情報は、そのセッションの際の認証（検証）、暗号化および応答の保護を強化するために用いられる。このモビィリティセキュリティアソシエーションは、無線サービスプロバイダによって加入の際に生成される。加入者がこのアソシエーションを修正することを許可するか否かは、無線サービスプロバイダに一任される。許される場合は、加入者は、顧客サービス係りに電話したり、secure Web site（セキュリティウエブサイト）にアクセスすることで、モビィリティセキュリティアソシエーションの内容を確認あるいは修正する。加えて、加入者は、サービスプロバイダによって許される他の加入者情報にアクセスすることもできる。

【０１９１】３．Modem MAC Address（モデムMACアドレス）。この欄は加入者によって所有されるモデムのMACアドレスを含む。登録の際に、共有のセキュリティに加えてこの欄もユーザを認証（検証）するために用いられる。このMACアドレスに基づく認証は、ユーザベースでオフすることもできる。このMACアドレスは登録の際にホーム登録サーバに送信される。

【０１９２】４．Enable MAC address Authentication（MACアドレス認証起動）。この欄は、MACアドレスに基づく認証が、enabled（起動）されているか、disabled（不能）にされているかを決定するために用いられる。enabled（起動）されている場合は、ホーム登録サーバは、登録を試みているエンドシステムのMACアドレスをこの欄に対してチェックすることで、エンドシステムの識別を検証する。disabled（不能）にされている場合は、このチェックは行なわれない。

【０１９３】５．Roaming Enabled Flag（ローミング起動標識）。この欄がenabled（起動）に設定されている場合は、エンドシステムは、フォーリンネットワークにローミングすることを許される。この欄がdisabled（不能）にされている場合は、エンドシステムは、フォーリンネットワークにローミングすることは許されない。

【０１９４】６．Roaming Domain List（ローミングドメインリスト）。この欄はRoaming Enabled Flagがenabled（起動 ）に設定されている場合にのみ意味を持つ。この欄は、エンドシステムがそこにローミングすることを許されるフォーリンドメインのリストを含む。このリストの内容がナル（空）で、しかも、Roaming Enabled Flagがenabled（起動 ）に設定されている場合は、そのエンドシステムは、自由にローミングすることを許される。

【０１９５】７．Service Enable/Disable Flag（サービス起動／不能標識）。この欄は、システム管理者によって、加入者へのサービスを不能にするためにdisabled（不能）に設定することができる。この欄がenabled（起動）に設定されている場合は、加入者はサービスを受けるために登録することを許される。加入者が登録した後に、この欄の値がdisabled（不能）に設定された場合は、その加入者のエンドシステムは、ネットワークによって即座に切断される。

【０１９６】８．Internet Service Provider Association（インターネットサービスプロバイダアソシエーション）。この欄は加入者のインターネットサービスプロバイダに関する情報を含む。この情報はIWFによって、P

PP登録フェーズの際に、エンドシステムに代わってインターネットサービスプロバイダを認証（検証）し、インターネットサービスプロバイダのPPPサーバとの間にL2TPトンネルを生成するために用いられる。この欄は加入者のISPの識別を含む。IWFは、この識別情報を用いて、エンドシステムに代わって認証とL2TPトンネルの設定を遂行するためにISPのディレクトリにアクセスする。

【０１９７】９．Subscriber's Name & Address Information（加入者の名前およびアドレス情報）。この欄は加入者の名前、アドレス、電話、ファックス、ｅ－メールアドレス等を含む。

【０１９８】ホームドメインディレクトリ（HDD）は、登録サーバによって、エンドシステムに代わって登録を完結するためにエンドシステムに関するパラメータを調べるために用いられる。登録サーバは、この情報を用いて、エンドシステムがホームから登録しているのか、あるいはそのエンドシステムがローミングエンドシステムであるかを決定する。ホームのエンドシステムである場合は、登録サーバはホーム登録サーバの役割を担い、エンドシステムの登録を行なう。ローミングエンドシステムである場合は、登録サーバはフォーリン登録サーバの役割を担い、Radius代理（プロキシ）として機能し、実際のホーム登録サーバの識別をこのディレクトリから調べ、そのホーム登録サーバに登録リクエストを転送する。このHDD内に格納されているローミングエンドシステムの場合に用いられるパラメータとしては、ホーム登録サーバのIPアドレス、ホームとフォーリンによって共有されるセキュリティ、ホームIWFとサービングIWFとの間のトンネルコンフィギュレーション等が含まれる。このHDDはMSC内に位置する。

【０１９９】このHDD内には以下の情報が格納されている：

１．Home Domain Name（ホームドメイン名）。この欄はエンドシステムによって登録リクエストに入れて供給された完全修飾ホームドメイン名と一致するHDD内のエントリを探すためのキーとして用いられる。

２．Proxy Registration Request（代理登録リクエスト）。この欄は登録サーバによってそれがフォーリン登録サーバとして機能すべきか否かを決定するために用いられる。真である場合は、フォーリン登録サーバとして機能し、エンドシステムの登録リクエストを実際のホーム登録サーバに中継する。

【０２００】３．Home Registration Server DNS Name（ホーム登録サーバのDNS名）。proxy registration request標識がTRUE（真）である場合は、フォーリン登録サーバは、この欄を用いて実際のホーム登録サーバのDNS名にアクセスする。真でない場合は、この欄は無視される。このDNS名はフォーリン登録サーバによってIPアドレスに翻訳される。フォーリン登録サーバはこのIPアドレスを用いて、エンドシステムの登録リクエストを中継する。

【０２０１】４．Foreign Domain Name（フォーリンドメイン名）。proxy registration request 標識がTRUE（真）である場合は、フォーリン登録サーバは、この欄を用いてフォーリンドメイン名に対応するエンドシステムのホーム登録サーバを識別する。真でない場合は、この欄は無視される。フォーリン登録サーバは、こうして得られた情報を用いて、フォーリンサーバマシンidをSMTPフォーマット、例えば、machine@fqdnの形式にて生成する。フォーリン登録サーバから、このマシンidをRadius-Access Reuestに挿入してホーム登録サーバに送信する。

【０２０２】５．Shared Secret（共有のセキュリティ）。proxy registration request 標識がTRUE（真）である場合は、この共有のセキュリティを用いて、フォーリン登録サーバとホーム登録サーバとの間で互いの識別が認証（検証）される。真でない場合はこの欄は無視される。

【０２０３】６．Tunneling Protocol Parameters（トンネリングプロトコルパラメータ）。この欄はエンドシステムにサービスを提供するためのトンネルを構成するために用いられる。ホームのエンドシステムに用いるパラメータとしては、基地局とホームIWFとの間、並びにホームIWFからPPPサーバへのトンネルに関する情報が含まれる。ローミングエンドシステムに用いるパラメータとしては、基地局からサービングIWFへの並びにサービングIWFからホームIWFへのトンネリングに関する情報が含まれる。この欄は各トンネルに対して、最小でも、用いるべきトンネリングプロトコルのタイプおよび任意のトンネリングプロトコルに特定なパラメータを含む。例えば、この欄はトンネリングプロトコルL2TPに対する識別子およびIWFとその相手（ピア）との間でL2TPトンネルを構成するために必要な追加のパラメータを含む。

【０２０４】７．Accounting Server Association（アカウンティングサーバアソシエーション）。この欄はIWFによってエンドシステムに代わってアカウンティングデータを生成するために必要な情報を格納するために用いられる。これには、アカウンティングプロトコルの名前（例えば、RADIUS）、アカウンティングサーバのDNS名およびそのアカウンティングプロトコルに固有のUDPポート番号等の追加のパラメータ、IWFがRadius Accountingプロトコル内に用いることを要求される共有のセキュリティ、チェックポインティングの頻度、セッション／マルチセッションidを生成するためのシード（種）等が含まれる。このアカウンティングサーバのDNS名は、アカウンティングサーバのIPアドレスに翻訳され、IWFに送信される。

【０２０５】互いにローミング合意を持つ無線サービスプロバイダの場合は、このHDDは、登録プロセスの認証（検証）および完結に用いられる。エンドシステムが自

身のホームネットワークからフォーリンネットワークにローミングした場合は、フォーリンネットワーク内のフォーリン登録サーバは、訪問してきたエンドシステムにサービスを提供する前に、自身のMSC内のHDDを調べ、訪問（ローミング）しているエンドシステムのホーム登録に関する情報を得てホームネットワークの認証（検証）を行なう。

【０２０６】ホームドメインディレクトリ管理に対するソフトウエアは、好ましくは、システム管理者に対して、グラフィカルユーザインタフェース（graphical user interface、GUI）に基づくHDD管理を提供する。システム管理者はこのGUIを用いてHDD内のエントリの確認や更新を行なう。ただし、このGUIはフォーリン無線ネットワークサービスプロバイダがローミング合意に基づいてリモートから更新を行なうためには意図されていない。これは、もっぱら、防火壁の内側で作業するホーム無線サービスプロバイダの信託された（トラステッド）従業員によって用いられることのみを意図される。

【０２０７】フォーリンドメインディレクトリ（FDD）は、ホームドメインディレクトリとは反対の機能を提供する。FDDはホーム登録サーバによって用いられる。つまり、ホーム登録サーバは、FDDからフォーリン登録サーバおよびフォーリンネットワークに関するパラメータを取り出し、フォーリンネットワークの認証（検証）やサービングIWFとホームIWFとの間のトンネルの生成の際にこれを用いる。これらパラメータには、ホームネットワークとフォーリンネットワークの間の共有のセキュリティや、ホームIWFとサービングIWFとの間のトンネルコンフィギュレーション等が含まれる。このFDDはホーム登録サーバのMSC内に位置する。このFDDはホーム登録サーバによってローミングエンドシステムの登録に用いられる。

【０２０８】このFDDには以下の情報が格納される：

１．Home Domain Name（ホームドメイン名）。この欄はエンドシステムを中継しているフォーリン登録サーバの完全修飾ドメイン名と一致するFDD内のエントリを探すためのキーとして用いられる。

２．Shared Secret（共有のセキュリティ）。これはフォーリン登録サーバとホーム登録サーバとの間で互いの識別を互いに認証（検証）するために用いられる共有のセキュリティである。

【０２０９】３．Home IFW-Serving IWF Tunneling Protocol Parameters（ホームIWFとサービングIWFの間のトンネリングプロトコルパラメータ）。この欄はホームIWFとサービングIWFとの間でトンネルを構成するために用いられる。この欄は、最小でも、用いるべきトンネリングプロトコルのタイプおよび任意のトンネリングプロトコルに特定なパラメータを含む。例えば、この欄はトンネリングプロトコルL2TPに対する識別子およびサービングIWFとホームIWFとの間でL2TPトンネルを構成するために必要な追加のパラメータを含む。

【０２１０】４．Accounting Server Association（アカウンティングサーバアソシエーション）。この欄はホームIWFによってエンドシステムに代わってアカウンティングデータを生成するために必要な情報を格納するために用いられる。これには、アカウンティングプロトコルの名前（例えば、RADIUS）、アカウンティングサーバのDNS名およびそのアカウンティングプロトコルに固有のUDPポート番号等の追加のパラメータ、IWFがRadius Accountingプロトコル内に用いることを要求される共有のセキュリティ、チェックポインティングの頻度、セッション／マルチセッションidを生成するためのシード（種）等が含まれる。このアカウンティングサーバのDNS名は、アカウンティングサーバのIPアドレスに翻訳され、IWFに送信される。

【０２１１】互いにローミング合意を持つ無線サービスプロバイダの場合は、このFDDは、登録プロセスの認証（検証）および完結に用いられる。エンドシステムが自身のホームネットワークからフォーリンネットワークにローミングした場合は、ホームネットワーク内の登録サーバは、自身のMSC内のFDDを調べ、エンドシステムにサービスを提供しているフォーリンネットワークに関する情報を得てフォーリンの認証（検証）を行なう。

【０２１２】このフォーリンドメインディレクトリ管理ソフトウエアは、好ましくは、システム管理者に対して、グラフィカルユーザインタフェース（GUI）に基づくFDD管理を提供する。システム管理者はこのGUIを用いてHDD内のエントリの確認や更新を行なう。ただし、このGUIはフォーリン無線ネットワークサービスプロバイダがローミング合意に基づいてリモートから更新を行なうためには意図されていない。これは、もっぱら、防火壁の内側で作業するホーム無線サービスプロバイダの信託された（トラステッド）従業員によって用いられることのみを意図される。

【０２１３】ホームIWFはインターネットサービスプロバイダディレクトリ（ISPD）を用いて、無線サービスプロバイダとサービス合意を持つISPとの間の接続性を管理し、加入者がそのネットワークを用いて自身のISPにアクセスできるようにする。各加入者に対して、加入者ディレクトリはその加入者のISPに対するエントリを持ち、この欄は、ISPD内のエントリをポイントする。ホームIWFはこの情報を用いて加入者に代わってISPへの接続を設定する。

【０２１４】このネットワークアーキテクチャはローミングをサポートする。複数の無線サービスプロバイダの間でローミングが機能するためには、このアーキテクチャは、無線サービスプロバイダ間のローミング合意の設定をサポートできる必要がある。このためには、２つの要件、つまり：（１）複数の無線サービスプロバイダを横断してシステムディレクトリを更新できること、およ

び（２）無線サービスプロバイダ間で請求書（料金）を清算できることが必要となる。

【０２１５】加入者がインターネットサービスプロバイダにアクセスできるようにするために、このネットワークアーキテクチャは、インターネットサービスプロバイダとの間にローミング合意を持つ。このためには、このネットワークアーキテクチャは、ISPのPPPサーバとの間でデータが授受できる必要がある（つまり、PPP、L2TP、Radius等の標準プロトコルをサポートできる必要がある）。このアーキテクチャはさらにISPアクセスに対するディレクトリの更新や、ISPとの間での料金の清算を扱える必要がある。

【０２１６】２つの無線サービスプロバイダの間でローミング合意が確立されると、両方のプロバイダは、他のネットワークからそのネットワークに訪問するエンドシステムに対する認証および登録機能をサポートするために、ホームおよびフォーリンドメインディレクトリを更新することが必要となる。本発明のネットワークアーキテクチャは、最小の場合は、手動のディレクトリ更新をサポートする。この方法においては、２つの無線サービスプロバイダの間でローミング合意が確立されると、合意した２つのパーティは、それらのホームおよびフォーリンドメインディレクトリに入力するための情報の交換を行なう。この方法では、これらディレクトリの実際の更新は、各サービスプロバイダの従業員によって手動で行なわれる。後になってホームおよびフォーリンドメインディレクトリ内の情報を更新することが必要になった場合は、合意した２つのパーティは、更新情報を交換し、これらの更新を手動でディレクトリに入力する。

【０２１７】代替の実施例においては、ディレクトリ管理ソフトウエアは、インターネットサービスプロバイダ間のローミングを可能にするとともに、ISPがローミング関係を自動的に管理および発見することを可能にするIETF標準の開発（developingstandards in IETF）を組み込む。この場合は、手動でのディレクトリ管理は不要となる。ネットワークシステムがローミング関係の伝搬、ローミング関係の発見、訪問するエンドシステムの認証および登録を自動的に遂行する。

【０２１８】アカウンティングデータの処理については、ネットワークアーキテクチャは、最小の場合は、単にアカウンティング情報の処理、格納、および無線サービスプロバイダの課金システムへのデータの送信のみをサポートし、ローミングに対する料金の清算は、課金システムに任される。

【０２１９】代替の実施例においては、インターネットサービスプロバイダの間にアカウンティングレコードを配送するIETF標準を開発（developing standards in IETF）がネットワークアーキテクチャ内に組み込まれ、ISPがローミングエンドシステムに対する料金の清算を行なうことが可能にされる。

【０２２０】システムソフトウエアは、ISPおよびプライベートイントラネットへのアクセスのサポートを、ホームIWFとISPのあるいはイントラネットのPPPサーバの間にL2TPをサポートすることで実現する。インターネットサービスプロバイダディレクトリ（ISPD）は、IWFがこれらトンネルを生成するために必要とされる情報を含む。無線サービスプロバイダとインターネットサービスプロバイダとの間でアクセス合意が行なわれると、このディレクトリは無線サービスプロバイダの従業員によって手動で更新される。無線サービスプロバイダとインターネットサービスプロバイダとの間のアクセス関係の自動的な更新および発見も現在開発されており、インターネット標準の進化に合わせて実現される見込みである。現時点ではインターネットサービスプロバイダにアクセスすると、加入者は２つの請求書を受け取る。つまり、第一は無線サービスプロバイダから無線ネットワークの使用に対して受け取り、第二はインターネットサービスプロバイダから受け取る。両方のタイプの料金を結合する（一つに纏める）共通の請求書は、この最小実現のソフトウエアでは扱われないが、将来的にはこのソフトウエアに料金清算のためのインターネット標準をこれらの進化に合わせて組み込み、加入者がISPと無線サービスプロバイダとの間のローミング合意に基づいて共通の請求書を受け取るようにすることも見込まれる。

【０２２１】システムはネットワーク要素を管理するための要素管理システムを含む。システム管理者は、要素マネージャから構成、性能および故障／警告管理機能を遂行する。要素管理アプリケーションは、ウエブブラウザ上でランする。ウエブブラウザを用いて、システム管理者はTCP/IPアクセスが可能な任意の場所からネットワークを管理する。要素マネージャは上位レベルのマネージャに対するエージェントの役割も遂行する。この役割の中で要素マネージャは警告および故障監視のためにSNMP MIB（Simple Network Manegement Protocol／Management Information Base）をエクスポートする。

【０２２２】上位レベルのSNMPマネージャは、SNMPトラップを介して警告状態を通知される。上位レベルのSNMPマネージャは定期的に要素マネージャのMIBにネットワークの健康（健全性）および状態について問い合せる。この上位レベルのSNMPマネージャの所のシステム管理者は、ネットワークのアイコンレプレゼンテーショ（アイコンによるネットワーク表現）とその現在の警告状態を監視することができる。特定のネットワーク要素アイコンをポイントし、クリックすることで、システム管理者は、ウエブブラウザを用いて要素管理アプリケーションを実行し、より細部の管理機能を遂行する。

【０２２３】ネットワーク内においては、物理的および論理的ネットワーク要素の管理は、SNMPプロトコルと内部管理用アプリケーションプログラミングインタフェースを用いて遂行される。要素マネージャ内のアプリケー

ションはSNMPあるいは他の管理API（Application Programming Interface）を用いてネットワーク管理機能を遂行する。

【０２２４】アーキテクチャ上は、要素管理システムには２つの異なるセットの機能要素が含まれる。第一のセットの機能要素には、コンフィギュレーションデータサーバ、パフォーマンスデータモニタ、健康／状態モニタ、およびネットワーク要素回復ソフトウエアが含まれ、これらはRAIDディスクを備えるHAサーバ上でランする。第二のセットの機能要素には、専用の非－HA管理システム上で実行する管理アプリケーションが含まれる。要素マネージャシステムが動作不能となった場合でも、これらネットワーク要素は引き続いてランし、警告を報告したり、さらには、故障状態を回復することができる。ただし、全ての管理アプリケーションは非－HAの要素マネージャ内で実行し、要素マネージャが故障した場合、人の介在を要求する回復動作は、要素マネージャが動作可能となるまでは不可能になる。

【０２２５】基地局内の無線ハブ（WH）は典型的には無線サービスプロバイダ（WSP）によって所有され、これらはWSPの登録サーバ（RS）にポイント・ツウ・リンク、イントラネット、あるいはインターネットによって接続される。WSPの登録サーバは、典型的には、プロセッサ上で実行し、幾つかの登録機能を遂行するソフトウエアモジュールである。インターワーキング機能ユニット（IWFユニット）は、典型的には、プロセッサ上で実行し、幾つかのインタフェーシング機能を遂行するソフトウエアモジュールである。IWFユニットは、典型的には登録サーバにイントラネット／WANを介して接続され、IWFユニットは典型的にはWSPによって所有される。ただし、IWFユニットは、必ずしも登録サーバと同一のLAN内に位置する必要はない。典型的には、アカウンティングサーバおよびディレクトリサーバは（プロセッサ上で実行するソフトウエアモジュールも含めて）登録サーバに、サービスプロバイダのデータセンタ（例えば、様々なサーバおよび他のソフトウエアをホストする一つあるいは複数のプロセッサを含むセンタ）内のLANを介して接続される。エンドシステムからのトラヒックは（このLANに接続された）ルータを介して公衆インターネットるいはISPのイントラネットにルートされる。フォーリンWSPのネットワーク内に位置する登録サーバはフォーリン登録サーバ（FRS）と呼び、エンドシステムのホームネットワーク（そのモバイルがそのサービスを購入する所のネットワーク）内に位置する登録サーバはホーム登録サーバ（HRS）と呼ぶ。また、ホームネットワーク内のインターネットワーキング機能ユニットはホームIWFと呼び、フォーリンネットワーク（つまりエンドシステムの訪問先のネットワーク）内のインターワーキング機能ユニットはサービングIWFと呼ぶ。

【０２２６】固定無線サービス（つまり、移動しないエンドシステム）の場合は、エンドシステムはホームネットワークのサービスを求めて、ホームネットワークから（例えば、アットホームサービス：at home service）、あるいはフォーリンネットワークから（例えば、ローミングサービス：roaming service）登録する。エンドシステムは無線ハブ内のエージェント（例えば、ソフトウエアにて実現されたエージェント機能）から送信されるアドバタイズメントをアクセスポイントを介して受信する。この際に、MAC層の登録とネットワーク層の登録の両方を遂行することが必要となる。

【０２２７】ホームに位置するエンドシステムの場合（図２３）は、ネットワーク層の登録（例えば、ローカルな登録）は、ホーム登録サーバにエンドシステムが現在接続されている無線ハブを知らせる。この場合は、エンドシステムのホームネットワーク内のIWFがアンカー、すなわちホームIWFとなる。こうしてエンドシステムとの間で授受されるPPPフレームは、無線ハブを介してホームネットワーク内のホームIWFに送られる。エンドシステムがホームに位置する場合、ホームIWFは無線ハブにXTunnelプロトコルを介して接続される。

【０２２８】フォーリンローミング無線サービスの場合（図２４）、フォーリン登録サーバは登録フェーズの際にローミングエンドシステムのホームネットワークの識別を見つける。この識別情報を用いて、フォーリン登録サーバはホーム登録サーバと通信し、エンドシステムの認証および登録を行なう。フォーリン登録サーバは、次に、サービングIWFを割り当て、ホームIWFとサービングIWFとの間にローミングエンドシステムのためにI-XTunnelプロトコル接続を確立する。サービングIWFは無線ハブとホームIWFとの間でフレームを中継する。ホームIWFからデータはPPPサーバ（つまり、ポイント・ツウ・ポイントプロトコルサーバ）に送られる。このPPPサーバは同一のIWF内に位置する場合もある。ただし、データが自身のPPPサーバを所有する企業イントラネットあるいはISPのイントラネットに向けられている場合は、データはL2TPプロトコルを介して別個のPPPサーバに送られる。この別個のサーバは、典型的には、無線サービスプロバイダとは別個のインターネットサービスプロバイダによって所有および運用される。ホームIWFとPPPサーバの位置はセッションを通じて固定されたままにとどまる。MAC層の登録とネットワーク層の登録を結合することで、MAC層の登録とネットワーク層の登録のために別個に要求されるオーバヘッドを節約することもできる。ただし、これら登録プロセスは結合しない方が、WSPの設備と純粋なIETF Mobile-IPをサポートする他の無線ネットワークとの相互運用性が確保でき便利である。

【０２２９】登録は、以下の３つのテーブルを設定する。テーブル１は、各アクセスポイントと関連する。テーブル１は各コネクション（例えば、各エンドシステム）をコネクションid（CID）にて識別し、コネクショ

ンidを特定の無線モデム（WM）のアドレス（つまり、エンドシステムのアドレス）と関連付ける。テーブル２は各無線ハブ（WH）と関連する。テーブル２は各コネクションidを対応する無線モデムアドレス、およびXTunnelのid（XID）と関連付ける。テーブル３は各インターワーキング機能（IWF）と関連する。テーブル３は各コネクションidを対応する無線モデムのアドレス、無線ハブのアドレス、XTunnelのid、およびIPポート（IP／ポート）と関連付ける。上述のテーブル内のエントリ（項目）は単にモビィリティ管理の説明に必要な項目のみを示し、実際には他にも重要なフィードが含まれることに注意する。

【０２３０】

【表１】

表１：ＡＰにおける接続テーブル

CID	WM
C1	WM1
C2	WM1
C1	WM2

表２：ＷＨにおける接続テーブル

CID	WM	AP	XID
C1	WM1	AP1	5
C2	WM1	AP1	5
C1	WM2	AP1	6
C1	WM3	AP2	7

表３：ＩＮＦにおける接続テーブル

CID	WM	WH	XID	IP/Port
C1	WM1	WH1	5	IP1/P1
C2	WM1	WH1	5	IP1/P2
C1	WM2	WH1	6	IP2/P3
C1	WM3	WH1	7	IP3/P1
C5	WM5	WH2	8	IP4/P1

【０２３１】図２５～２８は、ネットワーク内からダイアルフップするユーザ、並びに、ローミングユーザに対するプロトコルスタックを示す。図２５は、ホームの固定（つまり、移動しない）エンドシステムによる直接インターネットアクセスに対して用いるプロトコルスタックを示す。この構成では、PPPプロトコルメッセージはホームIWF（典型的には無線ハブと同一の位置に置かれる）に終端する。ホームIWFはメッセージをIPルータとの間で中継し、IPルータはメッセージをIWFと公衆インターネットの間で中継する。図２６は、ホームの固定（つまり、移動しない）エンドシステムによるリモートイントラネットアクセス（つまり、私設企業ネットあるいはISPへのアクセス）に対して用いるプロトコルスタックを示す。この構成では、PPPプロトコルメッセージはホームIWF（典型的には無線ハブと同一の位置に置かれる）を通じて私設企業イントラネットあるいはISPのPPPサーバに中継される。図２７は、フォーリンにローミングしているが固定の（つまり、移動していない）あるいは移動中のエンドシステムによる直接インターネットアクセスに対して用いられるプロトコルスタックを示す。この構成では、PPPプロトコルはホームIWF（典型的にはホームネットワークのモバイル交換センタ内に位置する）に終端し、ホームIWFは、IPルータとの間でメッセージを中継する。図２７に示すように、メッセージトラヒックはホームIWFに加えて、サービングIWF（典型的には無線ハブと同一の位置に置かれる）をも通ることに注意する。図２８は、フォーリンにローミングしているが固定の（つまり、移動していない）あるいは移動中のエンドシステムによるリモートイントラネットアクセス（つまり、私設企業ネットあるいはISPへのアクセス）に対して用いるプロトコルスタックを示す。この構成では、PPPプロトコルメッセージはホームIWF（典型的にはホームネットワークのモバイル交換センタ内に位置する）を通じて私設企業イントラネットあるいはISPのPPPサーバに中継される。図２８に示すようにメッセージトラヒックはホームIWFに加えて、サービングIWF（典型的には無線ハブと同一の位置に置かれる）をも通ることに注意する。サービングIWFと無線ハブがコンピュータの同一ネスト内に位置する場合、あるいは同一コンピュータ内にプログラムされている場合は、サービングIWFと無線ハブとの間にXTunnelプロトコルを用いてトンネルを設定する必要はない。

【０２３２】これらプロトコルスタックに対する同等な代替も可能である。例えば、RLPはサービングIWFあるいはホームIWF（モバイルがホームに位置する場合）に終端するのではなく、無線ハブに終端させることもできる。具体的には、IWFが無線ハブから遠く離れて位置し、パケットがIWFと無線ハブとの間の比較的損失が大きなIPネットワーク上を運ばれる場合は、RLPプロトコルは無線ハブの所に終端する方が好ましい。もう一つのバリエーションとしては、無線ハブとIWFの間のXtunnelは、必ずしもUDP/IPの上部に構築する必要がないことである。つまり、XtunnelはFrame Relay/ATM link層を用

いて構築することもできる。ただし、UDP/IPを用いた方が、無線ハブおよびIWFソフトウエアをあるネットワークから別のネットワークに移動するのが楽になる。

【０２３３】４つのタイプのハンドオフシナリオが発生することが考えられ、これらは、それぞれ、（ｉ）ローカルモビィリティ、（ii）マイクロモビィリティ、（iii）マクロモビィリティ、および（iv）グローバルモビィリティと呼ばれる。本発明の一つの実施例においては、これら４つの全てのシナリオにおいて、ルート最適化オプションは採用されず、ホーム登録サーバとISPのPPPサーバの位置は変更されない。ルート最適化を採用する本発明のもう一つの実施例においては、ISPのPPPサーバは変更されることがある。ただし、これについては後に説明する。加えて、フォーリン登録サーバとIWFの位置も最初の３つのシナリオにおいては変更されない。

【０２３４】勧告されているIETF Mobile IP標準は、エンドシステムがそれが接続されているIPサブネットを変更する場合は、必ず登録リクエストメッセージを自身のホームサブネット内のホームエージェントに送信することを要求する。このメッセージは新たなサブネット内でのエンドシステムとの連絡先である気付けアドレスを含む。トラヒックが、例えば、ISPからエンドシステムに向けて送信されると、ホームエージェントはこのエンドシステムに向けられたトラヒックを、これがホームサブネットに到着したとき傍受し、このトラヒックを気付けアドレスに転送する。この気付けアドレスはフォーリンサブネット内の特定のフォーリンエージェントを識別する。エンドシステムのフォーリンエージェントは、エンドシステム自身の中に駐在することも、トラヒックをエンドシステムに転送する別個のノード（つまり、代理登録エージェント）内に駐在することもある。Mobile IPのハンドオフにおいては、エンドシステムのエージェント、エンドシステムのホームエージェント、およびルート最適化オプションが採用される場合は対応するホスト（CH）の間で制御メッセージが交換される。

【０２３５】勧告されているIETF Mobile IP標準では、大きなインターネット内の全ての移動に対して目標とされる遅延およびスケーラビリティを満足することは困難である。本発明の階層化されたモビィリティ管理ではこれら目標を満足することができる。小さな移動（例えばアクセスポイントの変更）の場合は、MAC-層の再登録のみが必要とされる。大きな移動の場合は、ネットワーク層の再登録が遂行される。本発明による階層化されたモビィリティ管理は、IETFによって勧告されるMobile IP標準において用いられるフラットな構造とも、（Cellular Digital Packet Data forumによってスポンサされる標準に基づく）CDPD等のセルラシステムにおいて用いられるサービング／アンカーインターワーキング機能とも異なる。

【０２３６】図２９に示すように、ローカルモビィリティハンドオフは、同一の無線ハブに属するAP間のエンドシステム（mobile nodeの略であるMNとして示す）の移動を扱う。このため、MAC層の再登録のみが必要となる。エンドシステムは、新たなAPから無線ハブアドバタイズメントを受信し、この新たなAPに向けて登録リクエストを送り返す。

【０２３７】この新たなAP（つまり、エンドシステムから登録リクエストを受信したAP）は、自身のコネクションテーブル内に新たなエントリを生成し、登録メッセージを自身の無線ハブに中継する。ローカルモビィリティハンドオフにおいては、無線ハブは変更されない。無線ハブは、エンドシステムの登録リクエストを、MACレベルの登録リクエストであるものと認識し、無線ハブは自身のコネクションテーブルをこの新たなAPを反映するように更新する。次に、以前のAPは、自身のコネクションテーブルから以前のコネクションエントリを削除する。以前のAPがエントリを以前のエントリを削除するためには、少なくとも次の３つの方法、つまり、（ｉ）タイムアウトしたとき、（ii）新たなAPから無線ハブに中継されたMAC層アソシエーションメッセージのコピーを受信したとき（この中継メッセージがブロードキャストメッセージである場合）、あるいは（iii）無線ハブによるエントリを削除する旨の通知を受けたとき、に削除する方法がある。

【０２３８】図３０に示すように、マイクロモビィリティハンドオフは、同一の登録サーバに属する無線ハブ間のエンドシステム（mobile nodeの略であるMNとして示す）の移動で、かつ、エンドシステムが以前として現在のサービングIWFによって扱うことができる状況を扱う。アドバタイズメントが新たな無線ハブから（新たなAPを通じて）受信されると、エンドシステムは、その登録サーバへの登録をリクエストするメッセージを送信する。この登録リクエストは新たなAPと新たな無線ハブを通じてその登録サーバに中継される。

【０２３９】登録サーバは現在のIWFをまだ用いることができることを決定すると、登録サーバはbuild XTunnel Request message（XTunnel構築要請メッセージ）を現在のIWFに送ることで、現在のIWFに新たな無線ハブに向けてXTunnelを構築することを要請する。後に、登録サーバはtear down XTunnel Request message（XTunnel切断要請メッセージ）を現在のIWFに送ることで、現在のIWFに以前の無線ハブとの間の現在の XTunnelを切断することを要請する。このbuildおよびtear down XTunnel Request messageは一つのメッセージに結合することもできる。フォーリン登録サーバは、サービングIWFとホームIWFのいずれのIWFも変更されないために、登録メッセージをホーム登録サーバに転送することはない。

【０２４０】IWFからpositive build XTunnel reply（肯定的なXTunnel構築応答）およびpositive tear XTunnel reply（肯定的なXTunnel切断応答）を受信する

と、登録サーバはエンドシステムに登録応答を送り返す。登録応答が新たな無線ハブに到着すると、新たな無線ハブの所のコネクションテーブルが新たなAPへの接続を反映するために更新される。新たなAPは、新たな無線ハブからメッセージが受信され、登録応答がエンドシステムに送り返された後に、自身のMACフィルタアドレステーブルおよびコネクションテーブルを更新する。

【０２４１】次に、登録サーバは、relese message（開放メッセージ）を以前の無線ハブに送信する。以前の無線ハブは、relese messageを受信すると、自身のコネクションテーブルとMACフィルタアドレステーブルおよび以前のAPのコネクションテーブルを更新する。

【０２４２】図３１に示すように、マクロモビィリティハンドオフのケースは、フォーリンネットワーク内のサービングIWFは変更されるが、登録サーバは変更されない、無線ハブの間で移動を扱う。新たな無線ハブから（新たなAPを通じて）アドバタイズメントが受信されると、エンドシステムはネットワーク層の登録をリクエストするメッセージを登録サーバに向けて送信する。この登録リクエストは、新たなAPと新たな無線ハブを経て登録サーバに中継される。

【０２４３】登録サーバは、エンドシステムが現在の登録サーバのネットワークに属さない場合、自身がフォーリン登録サーバであると認識する。フォーリン登録サーバは、リクエスト、好ましくは、Radius Accessリクエスト（RAリクエスト）をフォーリンダイレクトリサーバ（大きなイエローページに類似）に送信することで、ホーム登録サーバの識別を見つけ、次に、適当なIWFをサービングIWFとして割り当て、その後、登録リクエスト、好ましくは、Radius Accessリクエスト（RAリクエスト）をホーム登録サーバに送信することで、ホーム登録サーバに新たに選択されたIWFを通知する。

【０２４４】ホーム登録サーバは、リクエスト、好ましくは、Radius Accessリクエスト（RAリクエスト）をホームダイレクトリサーバに送ることで、登録リクエストを認証（検証）する。登録リクエストが認証され、さらに、現在のホームIWFはまだ用いることができることが決定されると、ホーム登録サーバは、ホームIWFに対して、新たに割り当てられたサービングIWFに向けて新たなI-XTunnelを構築することと、以前のサービングIWFへの現在のI-XTunnelを切断することを指令する。ホームIWFからpositive buidld I-XTunnel replay（肯定的なI-XTunnel構築応答）およびpositive tear I-XTunnel reply（肯定的なI-XTunnel切断応答）を受信すると、ホーム登録サーバは、フォーリン登録サーバに登録応答を送り返す。

【０２４５】すると、フォーリン登録サーバは、新たに割り当てられたIWFに対して、新たな無線ハブに向けてXTunnelを構築することを指示する。positive buidld I-XTunnel replayを受信すると、フォーリン登録サーバは以前のIWFに対して、以前の無線ハブへのXTunnelを切断することを指令する。positive buidld I-XTunnel replayおよびpositive tear I-XTunnel replyを受信すると、フォーリン登録サーバはエンドシステムに登録応答を返信する。

【０２４６】登録応答が新たな無線ハブに到着すると、新たな無線ハブの所のコネクションテーブルが新たなAPへの接続を反映するように更新される。新たなAPは、新たな無線ハブからメッセージが受信され、登録応答がエンドシステムに送り返された後に、自身のMACフィルタアドレステーブルおよびコネクションテーブルを更新する。

【０２４７】次に、登録サーバはrelease message（開放メッセージ）を以前の無線ハブに送信する。無線ハブがrelease messageを受信すると、これは、自身のコネクションテーブルおよびMACフィルタアドレステーブルを更新し、以前のAPは、以前の無線ハブからメッセージを受信した後に自身のMACフィルタアドレステーブルおよびコネクションテーブルを更新する。

【０２４８】グローバルモビィリティハンドオフのケースは、登録サーバの変更を伴う無線ハブの間の移動を扱う。図３２はホームIWFは変更されない場合のグローバルモビィリティハンドオフを示し、図３３はホームIWFも変更される場合のグローバルモビィリティハンドオフを示す。新たなフォーリンネットワーク内の新たな無線ハブから（新たなAPを通じて）アドバタイズメントを受信すると、エンドシステムはネットワーク層の登録をリクエストするメッセージを新たなフォーリン登録サーバに送る。この登録リクエストは新たなAPと新たな無線ハブを経て新たなフォーリン登録サーバに中継される。

【０２４９】登録サーバは、エンドシステムが現在の登録サーバのネットワークに属さない場合、自身がフォーリン登録サーバであると認識する。フォーリン登録サーバは、リクエスト、好ましくは、Radius Accessリクエスト（RAリクエスト）をフォーリンダイレクトリサーバ（大きなイエローページに類似）に送信することで、ホーム登録サーバの識別を見つけ、次に、適当なIWFをサービングIWFとして割り当て、その後、登録リクエスト、好ましくは、Radius Accessリクエスト（RAリクエスト）をホーム登録サーバに送ることで、ホーム登録サーバに新たに選択されたIWFを通知する。

【０２５０】ホーム登録サーバは、リクエスト、好ましくは、Radius Accessリクエスト（RAリクエスト）をホームダイレクトリサーバに送ることで、登録リクエストを認証（検証）する。リクエストが認証され、現在のホームIWFをまだ用いることができることを決定すると（図３２）、ホーム登録サーバは、ホームIWFに対して、新たなフォーリン登録サーバによって新たに割り当てられたサービングIWFに向けて新たなI-XTunnelを構築することを指令する。ホーム登録サーバは、さらに、以

前のフォーリン登録サーバにde-registration message（登録解消メッセージ）を送信するとともに、ホームIWFに対して、以前のフォーリンネットワークの以前のサービングIWFへの以前のI-XTunnelを切断することを指令する。ホームIWFからpositive buidld I-XTunnel replay（肯定的なI-XTunnel構築応答）およびpositive tear I-XTunnel reply（肯定的なI-XTunnel切断応答）を受信すると、ホーム登録サーバはregistration reply（登録応答）を新たなフォーリン登録サーバに送る。

【０２５１】次に、新たなフォーリン登録サーバは、新たに割り当てられたIWFに対して、新たな無線ハブに向けてXTunnelを構築することを指令する。positive buidld XTunnel replay（肯定的なXTunnel構築応答）を受信すると、フォーリン登録サーバはエンドシステムに向けて登録応答を送り返す。この登録応答が新たな無線ハブに到着すると、新たな無線ハブの所のコネクションテーブルが新たなAPへの接続を反映するように更新される。新たなAPは、自身のMACフィルタアドレステーブルおよびコネクションテーブルを、新たな無線ハブからメッセージが受信され、登録応答がエンドシステムに転送された後に更新する。

【０２５２】次に、以前のフォーリン登録サーバは、以前のIWFに対して、以前の無線ハブへのXTunnelを切断するように指令する。positive tear XTunnel reply（肯定的なXTunnel切断応答）を受信すると、あるいはtear down XTunnel request（XTunnel切断リクエスト）を送信するのと同時に、以前のフォーリン登録サーバは、以前の無線ハブにrelease message（開放メッセージ）を送信する。以前の無線ハブがrelease messageを受信すると、これは、自身のコネクションテーブルおよびMACフィルタアドレステーブルを更新し、以前のAPは、自身のMACフィルタアドレステーブルおよびコネクションテーブルを以前の無線ハブからメッセージを受信した後に更新する。

【０２５３】他方、図３３に示すように、ホーム登録サーバが新たなフォーリン登録サーバからの登録リクエストは認証されたが、以前のホームIWFは用いることができないことが決定された場合は、ホーム登録サーバは新たなホームIWFを選択し、新たなホームIWFに対して、現在のPPPサーバ（例えば、接続されたISPイントラネット内のPPPサーバ）に向けて、レベル２トンネルプロトコルによるトンネル（つまりL2TPトンネル）を構築することを指令する。

【０２５４】次に、ホーム登録サーバは、以前のホームIWFに対して、そのL2TPトンネルトラヒックを新たなホームIWFに転送することを指令する。　次に、ホーム登録サーバは、新たなホームIWFに対して、新たなフォーリン登録サーバによって新たに割り当てられたサービングIWFに向けて新たなI-XTunnelを構築することを指令する。ホーム登録サーバは、さらに、de-registration message（登録解消メッセージ）を以前のフォーリン登録サーバに送信するとともに、ホームIWFに対して、以前のフォーリンネットワークの以前のサービングIWFへの以前のI-XTunnelを切断することを指令する。ホームIWFからpositive buidld I-XTunnel replay（肯定的なI-XTunnel構築応答）およびpositive tear I-XTunnel reply（肯定的なI-XTunnel切断応 答）を受信すると、ホーム登録サーバは登録応答を新たなフォーリン登録サーバに送信する。

【０２５５】すると、新しいフォーリン登録サーバは、新たに割り当てられたIWFに対して、新たな無線ハブへのXTunnelを構築することを指令する。positive build XTunnel replay（肯定的なXTunnel構築応答）を受信すると、フォーリン登録サーバはエンドシステムに向けて登録応答を送り返す。登録応答が新たな無線ハブに到着すると、無線ハブの所のコネクションテーブルが新たなAPへの接続を反映するように更新される。新たなAPは、自身のMACフィルタアドレステーブルおよびコネクションテーブルを、新たな無線ハブからメッセージが受信され、登録応答がエンドシステムに転送された後に更新する。

【０２５６】以前のフォーリン登録サーバは、以前のIWFに対して、以前の無線ハブへのXTunnelを切断することを指令する。positive tear XTunnel reply（肯定的なXTunnel切断応答）を受信するとあるいはtear down XTunnel reques（XTunnel切断要請）を送信するのと同時に、以前のフォーリン登録サーバはrelease message（開放メッセージ）以前の無線ハブに送信する。以前の無線ハブは開放メッセージを受信すると、自身のコネクションテーブルおよびMACフィルタアドレステーブルを更新し、以前のAPは、自身のMACフィルタアドレステーブルおよびコネクションテーブルを以前の無線ハブからメッセージを受信した後に更新する。

【０２５７】本発明に従って構成されたエンドシステムはIETFが勧告するMobile-IP標準に従って構成されたネットワークと相互に動作でき、IETFが勧告するMobile-IP標準に従って構成されたエンドシステムも本発明に従って構成されたネットワークと相互に動作できる。

【０２５８】本発明のネットワークとIETF Mobile-IP（rfc2002、標準ドキュメント）との主な差異は以下の通りである：

（ｉ）本発明がモビィリティ管理のために階層概念を用いるのに対して、IETFが勧告するMobile-IP標準は、フラットな構造を用いる。本発明のネットワークにおいては、小さなエリア内での小さなモビィリティ（ハンドオフ）に対しては、ネットワークレベルの登録は必要とされない。マイクロモビィリティは、新たなXtunnelの設定と以前のXtunnelの切断を伴う。グローバルモビィリティは、最小でも、XTunnelの設定／切断に加えて、新たなI-XTunnelの設定と以前のI-XTunnelの切断を伴う。

グローバルモビィリティは、新たなL2TP Tunnelの設定および以前のL2TP Tunnelから新たなL2TP TunnelへのL2TP状態の転送を伴う。

【０２５９】（ii）本発明は、リモートダイヤルアップユーザを識別するために、ユーザ名＋領域（realm）を用いるにの対して、IETFが勧告するMobile-IP標準は固定ホームアドレスを用いる。

（iii）本発明では登録機能とルーティング機能は別個のエンティティによって遂行される。これら２つの機能はIETFが勧告するMobile-IP標準ではホームエージェントによって遂行され、両方の機能はIETFが勧告するMobile-IP標準ではフォーリンエージェントによっても遂行される。これにと対象的に、本発明の一つの実施例においては、登録機能は登録サーバによって遂行され、ルーティング機能は、ホームIWFとフォーリンIWFの両方および無線ハブ（アクセスハブとも呼ばれる）によって遂行される。

【０２６０】（iv）本発明は、PPPセッション当たり３つのトンネルを用いる。XTunnelは、無線ハブとサービングIWFとの間のlink-layer tunnel（リンク層トンネル）により近い。サービングIWFとホームIWFとの間のI-XTunnelは、IETFが勧告するMobile-IP標準のホームとフォーリンエージェントとの間のトンネルにより近い。L2TPトンネルはホームIWFがPPPサーバでない場合にのみ用いられる。

【０２６１】（v）本発明では、ネットワーク層の登録はPPPセッションが開始される前に発生するのに対して、IETFが勧告するMobile-IP標準では、Mobile-IPの登録は、PPPセッションがオープン状態に入った後に発生する。

（vi）本発明では、エージェントアドバタイズメントをアドバタイズするネットワークエンティティ（つまり、無線ハブ）は、エンドシステムへの直接リンク上には存在しないのに対して、IETFが勧告するMobile-IP標準では、エージェントアドバタイズメントは、TTL of 1（１のTTL）を持つことが要求され、これはエンドシステムがフォーリンエージェントと直接リンクを持つことを意味する。加えて、本発明のエージェントアドバタイズメントは、IETFが勧告するMobile-IP標準の場合のようなICMPルータアドバタイズメントに対する拡張ではない。

【０２６２】本発明によるエンドシステムはエージェント請求（agent solicitation）をサポートすることを要求される。本発明によるエンドシステムが、IETFが勧告するMobile-IP標準をサポートするネットワークを訪問した場合、エンドシステムはエージェントアドバタイズメントが送られているのを待つ（聞こえるのを待つ）。もし、エンドシステムが、エージェントアドバタイズメントを妥当な時間フレーム内に受信しない場合、エンドシステムはエージェント請求（agent solicitation）をブロードキャストする。

【０２６３】本発明においては、ネットワーク運用者は、IETFが勧告するMobile-IP標準をサポートする他のネットワークと、それら他のネットワークを用いることを希望する本発明によるエンドシステムにホームアドレスを割り当てられるように協議することができる。本発明のエンドシステムは、エージェントアドバタイズメントを受信したとき、それが訪問しているネットワークが本発明によるネットワークではないことを決定し、登録のためにこうして割り当てられたホームアドレスを用いることができる。

【０２６４】IETFが勧告するMobile-IP標準をサポートするネットワークの場合は、PPPセッションが、Mobile-IPの登録の前に開始され、PPPサーバはそれらのネットワーク内のフォーリンエージェントと同一の位置にあるものと想定される。一つの実施例においては、SNAPヘッダを用いてPPPフレームが本発明のMACフレームに（Ethernetフォーマットと類似する方法にて）カプセル化され、フォーリンエージェントはこのフォーマットをproprietary PPP format over Ehthernet encapsulationであると解釈する。こうして、本発明によるエンドシステムと相手のPPPはオープン状態に入ることができる。その後、フォーリンエージェントは、エージェントアドバタイズメントの送信を開始し、本発明のエンドシステムは登録が可能となる。

【０２６５】IETFが勧告するMobile-IP標準をサポートするエンドシステムが本発明のタイプのネットワーク内で動作できるようにするためには、これらモバイル（エンドシステム）は少なくとも類似のMAC層の登録を遂行できることが必要とされる。本発明のエージェントアドバタイズメントメッセージのフォーマットをIETFが勧告するMobile-IP標準のエージェントアドバタイズメントメッセージのフォーマットと類似させることで、本発明のネットワークに訪問するエンドシステムは、エージェントアドバタイズメントを解釈し、無線ハブに登録することが可能となる。本発明の登録リクエストおよび応答メッセージは、IETFが勧告するMobile-IP標準の登録リクエストおよび応答メッセージに（不要な拡張なしに）類似し、このため、本発明のモビィリティ管理機能の他の部分は、本発明のネットワークに訪問するエンドシステムに透過的である。

【０２６６】IETFが提唱するMobile-IP標準をサポートするエンドシステムはMobile-IP登録の前にPPPセッションが開始されることを期待するために、本発明の無線ハブは、オプションとして、MAC-層の登録の後にPPPのLCP（Link control Protocok）パケットおよびNCP（Network Control Protocol）パケットの解釈を開始することもできる。

【０２６７】ハンドオフの際にトラヒックが失われるのを回避するために、本発明のモビィリティ管理は、メークビフォアブレーク（make before break）という概念

を用いる。ローカルモビィリティの場合は、メークビフォアブレークコネクション（make before break connection）は、新たなAPによって無線ハブに中継されるMAC-層登録メッセージをブロードキャスメッセージに変換することによって達成される。こうして、以前のAPは、新たな登録を聞くことができ、エンドシステムに向けられたまだ伝送されてないパケットを新たなAPに転送することが可能となる。

【０２６８】マイクロモビィリティの場合は、新たな無線バブに関する情報がサービングIWFと以前の無線ハブとの間で交換されるTear XTunnelメッセージ内に挿入される。こうして、以前の無線ハブは、サービングIWFからのTear XTunnelメッセージを聞いたときに、緩衝したパケットを新たな無線ハブに転送することが可能となる。

【０２６９】同時に、WIFの所のRLP層がそれまでに以前の無線ハブから確認応答のあったシーケンス番号を覚えている方法である。同時に、IWFも、以前の無線ハブに送られた最も新しいパケットの現在の送信シーケンス番号（current send sequencenumber）を覚えている。こうして、IWFは、これら２つの番号の間に来るパケットを、新たな無線ハブに、より新たなパケットを新たな無線ハブに送信する前に送信することが可能となる。RLP層は重複パケットをフィルタできるものと想定される。第二のアプローチの方が、以前の無線ハブは互いに直接に通信できないと考えられるために、第一のアプローチよりも好ましい。

【０２７０】マクロモビィリティの場合は、以前の無線ハブから新たな無線ハブへのパケット転送に加えて、以前のサービングIWFがパケットを新たなサービングIWFに転送する。これを達成するためには、単に、新たなサービングIWFの識別をtear downI-XTunnelメッセージに挿入して新たなサービングIWFに送ることのみが必要とされる。これと同一の結果を達成するためのもう一つの方法として、ホームIWFは、以前のサービングIWFによって最後に確認応答のあったI-XTunnelのシーケンス番号と、ホームIWFによって送信された現在のI-XTunnelのシーケンス番号を知っているために、以前のサービングIWFが損失パケットを新たなサービングIWFに転送するのでなくホームIWFがこの仕事を遂行する方法である。

【０２７１】ハンドオフの間でのトラヒック損失を最小にするためにどれだけの量のバッファを、それぞれ、モバイル当たり／AP当たり／無線ハブ当たり／IWF当たりに割り当てるかを推定する一つの方法としては、エンドシステム当たり／AP当たり／無線ハブ当たり／IWF当たりのパケット到着速度とハンドオフ時間を推定する方法がある。この情報をIWFの無線ハブの以前のAPにパスすることで、ハンドオフ時に、それぞれ、IWFの無線ハブの新たなAPにどの程度のトラヒックが転送されるべきか決定される。

【０２７２】本発明においてルートの最適化を達成するためには、エンドシステムはサービングIWFに最も近いPPPサーバを選択する。ルート最適化なしでは、過剰な輸送遅延や過剰な物理リンクの使用が発生することがある。

【０２７３】例えば、ニューヨーク市内のホームネットワークに加入するエンドシステムが香港にローミングするものと想定する。香港のISPにリンクを設定するためには、エンドシステムは、香港内の無線ハブ内に設定されたサービングIWFと、ニューヨーク市内のホームネットワーク内に設定されたホームIWFとを持つこととなる。この場合、メッセージは、（香港にローミングした）エンドシステムから（香港内の）サービングIWFに向かい、ここから（ニューヨーク市内の）ホームIWFを経て、再び、香港のISPに戻るようにルートされる。

【０２７４】一つの好ましいアプローチは（香港内の）サービングIWFを直接に香港のISPに接続する方法である。この場合は、サービングIWFがホームIWFのように機能する。この実施例においては、前提として、ホームとフォーリン無線プロバイダの間にローミング合意が存在する。加えて、課金情報が共有されるようにさまざまなアカウンティング／課金システムが互いに自動的に通信するようにされる。アカウンティングおよび課金情報の交換はIETFのROAMOPS作業グループによって勧告される標準等を用いて実現する。

【０２７５】ただし、サービングIWFは、この場合でも、最も近いPPPサーバ（例えば、香港のISP）を見つけることを必要とされる。現在の実施例においては、フォーリン登録サーバはエンドシステムのPPPサーバ（例えば、香港のISP）への接続の希望をフォーリン登録サーバがエンドシステムから登録リクエストを受信したときに知る。フォーリン登録サーバがサービングIWFの方が要求されるPPPサーバ（例えば、香港のISP）にホームIWFよりも近いことを知ると、フォーリン登録サーバはサービングIWFに対して、L2TPトンネルを（ホーム登録サーバおよびホームIWFに最も近いPPPサーバではなく）自身に最も近いPPPサーバに向けて確立することを指令する。次に、フォーリン登録サーバは、ホーム登録サーバにエンドシステムがサービングIWFとフォーリンPPPによるサービスを受けている事実を通知する。

【０２７６】もう一つの実施例においては、フォーリン登録サーバはサービングIWFの方が希望されるPPPサーバ（例えば、香港のISP）にホームIWFより近いことを、フォーリン登録サーバがエンドシステムから登録リクエストを受信したときに知る。すると、フォーリン登録サーバは登録リクエストメッセージにサービングIWFの情報を示すメッセージとルート最適化が要望されることを示す通知とを付加して、これをホーム登録サーバに送る。同時にフォーリン登録サーバはサービングIWFに対して、L2TPトンネルをPPPサーバに向けて確立することを

指令する。登録リクエストが承認された時点で、ホーム登録サーバはホームIWFに対してL2TPの状態をフォーリンIWFに転送するように指令する。

【0277】図34においては、データフレームは、最初は、第一のモバイルエンドシステムと、第一のアクセスポイントを通じて第一のアクセスハブとの間で通信されている。次に、第一のモバイルエンドシステムが移動し、第二のアクセスポイントを通じて再登録するとき、登録リクエストが第一のモバイルエンドシステムから第二のアクセスポイントを通じて第一のアクセスハブに送信され、第一のモバイルエンドシステムが第一のアクセスハブに、第一の登録サーバに通知することなく、再登録される。最後に、第一のモバイルエンドシステムが第二のアクセスポイントを通じて再登録されたとき、第二のアクセスポイントが第一のアクセスハブとリンクされ、第二のアクセスポイントが第一のアクセスハブとリンクされたとき、第一のアクセスポイントと第一のアクセスハブとのリンクが切断される。

【0278】図35においては、データフレームは、最初は、第一のモバイルエンドシステムと、第一のアクセスハブを通じて第一のインターワーキング機能（IWF）との間で通信されている。次に、第一のモバイルエンドシステムが移動し、第二のアクセスハブを通じて再登録するとき、登録リクエストが第一のモバイルエンドシステムから第一のアクセスポイントおよび第二のアクセスハブを通じて第一の登録サーバに送信され、第一のモバイルエンドシステムが、ホーム登録サーバに通知することなく、第一の登録サーバに再登録される。最後に、第一のモバイルエンドシステムが第二のアクセスハブを通じて再登録されたときに、第二のアクセスハブが第一のインターワーキング機能とリンクされ、第二のアクセスハブが第一のインターワーキング機能とリンクされた後に、第一のアクセスハブと第一のインターワーキング機能との間のリンクが削除される。

【0279】図36においては、フォーリンネットワークにおいては、データフレームは、最初は、第一のモバイルエンドシステムと、第一のインターワーキング機能を通じて第三のインターワーキング機能との間で通信されており、ホームネットワークにおいては、データフレームは、最初は、第三のインターワーキング機能と第一の通信サーバとの間で通信されている。次に、第一のモバイルエンドシステムが移動し、第一のアクセスハブを通じて再登録するとき、登録リクエストが第一のモバイルエンドシステムから第一のアクセスポイント、第一のアクセスハブ、および第一の登録サーバを通じてホーム登録サーバに送信され、第一のモバイルエンドシステムがホーム登録サーバに、第三のインターワーキング機能と第一の通信サーバとの間のリンクを切断することなく、再登録される。第一の登録サーバから登録リクエストをホーム登録サーバに送信するステップにおいて、第一のインターワーキング機能から第二のインターワーキング機能に変更する指標が送られる。最後に、第一のモバイルエンドシステムが第一のアクセスハブを通じて再登録されたとき、第二のインターワーキング機能が第三のインターワーキング機能とリンクされ、第二のインターリンク機能が第三のインターワーキング機能とリンクされた後に、第一のインターワーキング機能と第三のインターキング機能との間のリンクが切断される。

【0280】図37においては、第一のフォーリンネットワークにおいては、データフレームは、最初は、第一のモバイルエンドシステムと第一のインターワーキング機能を通じて第三のインターワーキング機能との間で通信されており、ホームネットワークにおいては、データフレームは、最初は、第三のインターワーキング機能と第一の通信サーバとの間で通信されている。次に、第一のモバイルエンドシステムが移動し、第一のアクセスハブを通じて再登録するとき、登録リクエストが第一のモバイルエンドシステムから第一のアクセスポイント、第一のアクセスハブ、および第二の登録サーバを通じてホーム登録サーバに送信され、第一のモバイルエンドシステムがホーム登録サーバに、第三のインターワーキング機能と第一の通信サーバとの間のリンクを切断することなく、再登録される。最後に、第一のモバイルエンドシステムが第一のアクセスハブを通じて再登録されたとき第三のインターワーキング機能が第二のインターワーキング機能とリンクされ、第三のインターワーキング機能が第二のインターワーキング機能とリンクされた後に、第三のインターワーキング機能と第一のインターワーキング機能との間のリンクが切断される。

【0281】図38においては、フォーリンネットワークにおいては、データフレームは、最初は、第一のモバイルエンドシステムと、第一のインターワーキング機能を通じて第三のインターワーキング機能との間で通信されており、ホームネットワークにおいては、データフレームは最初は、第三のインターワーキング機能と第一の通信サーバとの間で通信されている。次に、第一のモバイルエンドシステムが移動し、第一のアクセスハブを通じて再登録するとき、登録リクエストが第一のモバイルエンドシステムから第一のアクセスポイント、第一のアクセスハブ、および第二の登録サーバを通じてホーム登録サーバに送られ、第一のモバイルエンドシステムがホーム登録サーバに再登録される。最後に、第一のモバイルエンドシステムが第一のアクセスハブを通じて再登録されると、第四のインターワーキング機能と第二のインターワーキング機能がリンクされ、第四のインターワーキング機能が第一の通信サーバとリンクされ、第四のインターワーキング機能が第一の通信サーバとリンクされたとき第三のインターワーキング機能と第一の通信サーバとの間のリンクが切断され、第四のインターワーキング機能が第二のインターワーキング機能とリンクされた

後に、第三のインターワーキング機能と第一のインターワーキング機能との間のリンクが切断される。

【0282】本発明による無線データネットワークは、ホームモバイル交換センタ、フォーリンモバイル交換センタ、基地局、およびエンドユーザを含む。ホームモバイル交換センタは、ホーム登録サーバとホームインターワーキング機能を含む。フォーリンモバイルセンタは、サービング登録サーバとサービングインターワーキング機能を含む。基地局は、代理（プロキシ）登録エージェントを含む。エンドユーザのモデムは、ユーザ登録エージェントを含む。ユーザ登録エージェントは代理登録エージェントに結合され、代理登録エージェントはサービング登録エージェントに結合され、サービング登録サーバはホーム登録サーバに結合される。代理登録エージェントは、ユーザ登録エージェントから要求（solicitation）メッセージを受信したとき気付けアドレスを含むアドバタイズメントを送信するモジュールを含み、ユーザ登録エージェントは、ユーザ登録エージェントがアドバタイズメントを受信したときユーザ識別情報および気付けアドレスを、登録リクエスト内に組み込むためのモジュール、およびこの登録リクエストを代理登録エージェントに送信するためのモジュールを含む。代理登録エージェントは、任意のユーザから受信される任意の登録リクエストをサービング登録エージェントに転送するためのモジュールを含む。サービング登録サーバは、ホーム登録サーバのアドレスを見つけるためのフォーリンディレクトリモジュール、ホーム登録サーバのアドレスが見つかったとき登録リクエストをカプセル化し、サービング登録サーバの識別情報を組み込み、カプセル化された登録リクエストをRadiusアクセスリクエストに組み込むためのモジュール、およびRadiusアクセスリクエストをホーム登録サーバに送信するためのモジュールを含む。ホーム登録サーバは、サービング登録サーバの識別情報を認証（検証）するためのホームディレクトリモジュール、サービング登録サーバの識別情報が認証されたときRadiusアクセスリクエストからインターワーキング機能リクエストを形成するためのモジュール、およびインターワーキングリクエストをホームインターワーキング機能に送信するためのモジュールを含む。

【0283】無線エンドユーザがローミングできる新規のネットワークアーキテクチャの幾つかの好ましい実施例について説明したが、これらは単に説明を意図するもので、制限を加えることを意図するものではなく、当業者においては上述の教示に照らして様々な修正およびバリエーションを考えることができると思われる。例えば、ここで説明された接続リンクには、周知の接続プロトコル（例えば、IP、TCP/IP、L2TP、IEEE 802.3等）を用いて設定されるが；ただし、本発明から逸脱することなく、他の接続プロトコルを用いて同一あるいは類似のデータ配信能力を持つ接続リンクを設定することも可能である。上述の様々な実施例における動作エージェント（acting agent）は、ソフトウエアによって制御されるプロセッサの形式を取ることも、他の制御の形式（例えば、プログラマブル論理アレイ等）を取ることもできる。動作エージェントは説明のようにグループ化することも、あるいは、説明の接続方法から逸脱することなく、上述のセキュリティおよび認証方法を達成できることを条件に、別の仕方にグループ化することもできる。さらに、単一の、アクセスポイント、アクセスハブ（つまり無線ハブ）あるいはインターワーキング機能ユニット（IWFユニット）にて、マルチチャネル能力を提供することもできる。このため、単一の、アクセスポイント、アクセスハブあるいはIWFユニットにて複数のエンドシステムからのトラヒッを扱うこともでき、従って、ここでは別個の複数の、アクセスポイント、アクセスハブあるいはＩＷＦユニットとして説明されたものと同一なものを、単一のマルチチャネル、アクセスポイント、アクセスハブあるいはＩＷＦにて実現することもできる。従って、開示された本発明の幾つかの特定な実施例に対して、特許請求の範囲によって定義される本発明の範囲および精神から逸脱することなく、様々な変更を加えることができるものである。

【図面の簡単な説明】

【図１】公衆交換電話ネットワークを通じての周知のリモートアクセスアーキテクチャの構成図である。

【図２】本発明による無線パケット交換データネットワークを通じてのリモートアクセスアーキテクチャの構成図である。

【図３】図２のネットワークのアーキテクチャのローミングシナリオを示す選択された部分の構成図である。

【図４】ローカルアクセスポイントを持つ基地局の構成図である。

【図５】リモートアクセスポイントを持つ基地局の構成図である。

【図６】リモートアクセスポイントを持つ基地局であって、幾つかのリモートアクセスポイントが無線トランク接続を用いて接続される構成図である。

【図７】ローカルアクセスポイントに対するプロトコルスタックの図である。

【図８】無線トランクを持つリモートアクセスポイントに対するプロトコルスタックの図である。

【図９】リモートアクセスポイントを無線トランクにてサポートするための基地局内の中継機能に対するプロトコルスタックの図である。

【図１０】図９に示す中継機能を実現するためのプロトコルスタックの図である。

【図１１】ローカルアクセスポイントをサポートするための基地局内の中継機能に対するプロトコルスタックの図である。

【図１２】図２のネットワークのアーキテクチャの選択

された部分の構成図であって、ホームネットワークからホームネットワークに登録する第一のエンドシステムと、フォーリンネットワークからホームネットワークにホームインターワーキング機能をアンカーとして用いて登録する第二のエンドシステムを示す。

【図１３】図２のネットワークのアーキテクチャの選択された部分の構成図であって、ホームネットワークからホームネットワークに登録する第一のエンドシステムと、フォーリンネットワークからホームネットワークにサービングインターワーキング機能をアンカーとして用いて登録する第二のエンドシステムを示す。

【図１４】フォーリンネットワークからホームネットワークに登録するため、および、データリンクを、確立、認証、および構成するために用いるリクエストおよび応答メッセージの梯子図である。

【図１５】図２のネットワークのアーキテクチャの選択された部分の構成図であって、モバイルをホームネットワークからホームネットワークに登録する際の登録リクエストおよび応答を示す。

【図１６】図２のネットワークのアーキテクチャの選択された部分の構成図であって、モバイルをフォーリンネットワークからホームネットワークに登録する際の登録リクエストおよび応答を示す。

【図１７】ホームネットワーク内のエンドシステムとホームネットワーク内のインターワーキング機能との間の通信であって、セルサイトがローカルアクセスポイントを持つ場合のプロトコルスタックの構成図である。

【図１８】ホームネットワーク内のエンドシステムとホームネットワーク内のインターワーキング機能との間の通信であって、セルサイトが無線トランクを通じて無線ハブに接続されたリモートアクセスポイントを持つ場合のプロトコルコルスタックの構成図である。

【図１９】ローミングエンドポイントに結合された基地局とホームインターワーキング機能との間の通信を示すプロトコルスタックの構成図である。

【図２０】ホームネットワーク内のエンドシステムがホームネットワーク内のインターワーキング機能を通じてインターネットプロトコルプロバイダに接続する場合の通信を示すプロトコルスタックの構成図である。

【図２１】フォーリンネットワーク内のエンドシステムとホームネットワーク内のホーム登録サーバとの間の登録フェーズの際の通信を示すプロトコルスタックの構成図である。

【図２２】アカウンティングデータを顧客課金システムに送るまでの処理を示す処理流れ図である。

【図２３】ホームネットワーク内のエンドシステムに対する登録プロセスを示す梯子図である。

【図２４】フォーリンネットワーク内のエンドシステムに対する登録プロセスを示す梯子図である。

【図２５】PPPプロトコルがホームネットワークのインターワーキングに終端する場合のホームネットワーク内のエンドシステムの接続を示すプロトコルスタック図である。

【図２６】PPPプロトコルがISPあるいはイントラネットに終端する場合の、ホームネットワーク内のエンドシステムの接続を示すプロトコルスタック図である。

【図２７】PPPプロトコルがフォーリンネットワークのインターワーキング機能に終端する場合のフォーリンネットワーク内のエンドシステムの接続を示すプロトコルスタック図である。

【図２８】PPPプロトコルがISPあるいはイントラネットに終端する場合のフォーリンネットワーク内のエンドシステムの接続を示すプロトコルスタック図である。

【図２９】ローカルハンドオフシナリオを示す梯子図である。

【図３０】フマイクロハンドオフシナリオを示す梯子図である。

【図３１】マクロハンドオフシナリオを示す梯子図である。

【図３２】グローバルハンドオフシナリオであって、フォーリン登録サーバは変更されるが、ホームインターワーキング機能は変更されない場合を示す梯子図である。

【図３３】グローバルハンドオフシナリオであって、フォーリン登録サーバとホームインターワーキング機能の両方が変更される場合を示す梯子図である。

【図３４】本発明によるローカル手続きを示す機能流れ図である。

【図３５】本発明によるマイクロ手続きを示す機能流れ図である。

【図３６】本発明によるマクロハンドオフ手続きを示す機能流れ図である。

【図３７】本発明によるグローバルハンドオフ手続きであって、ホームネットワーク内のインターワーキング機能は変更されない場合を示す機能流れ図である。

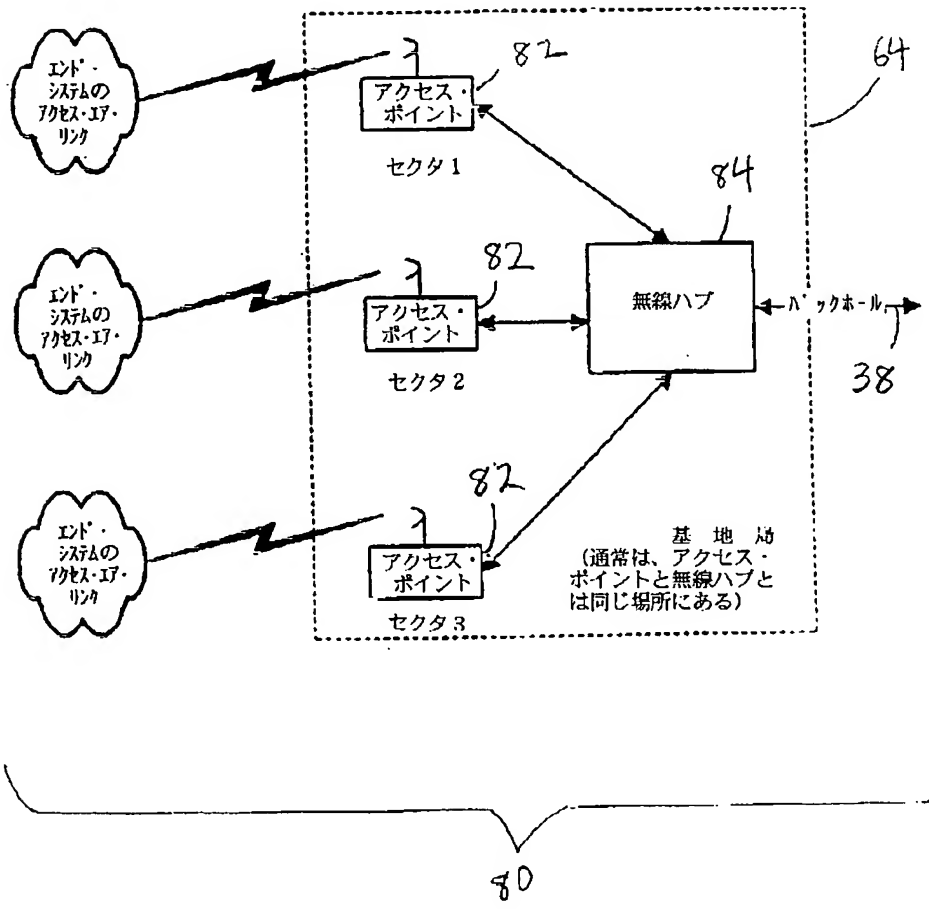
【図３８】本発明によるグローバルハンドオフ手続きであって、ホームネットワーク内のインターワーキング機能が変更される場合を示す機能流れ図である。

【符号の説明】

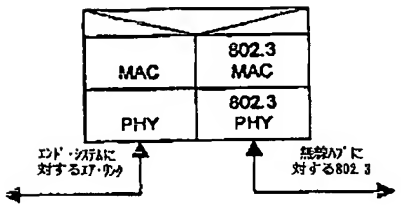
４　ユーザモデム
２　ユーザコンピュータ
８　ポイントオブプレゼンス（POP）
１０　イントラネットバックボーン
１４　メディアデータセンタ
１２　ルータ
１８　ペライベートイントラネット
２０　公衆インターネットバックボーン
３０　無線ネットワーク
３２　エンドシステム
３４　エアリンク
３６　基地局

38　バックホールネットワーク
40　モバイル交換センタ（MSC）
42　IPルータ
44　公衆インターネット
46　プライベートイントラネット
46　インターネットサービスプロバイダ
48　アカウンティングおよびディレクトリサーバ
50　要素管理サーバ
52　パケットデータインタワーキング機能（IWF）
60　ローミングエンドシステム
62　フォーリン無線サービスプロバイダ
64　基地局
66　サービングIWF
70　ホーム無線サービスプロバイダ
72　ホームIWF
74　インターネットサービスプロバイダ
80　無線サブネットワーク
82　アクセスポイント
84　無線ハブ
86　無線トランク

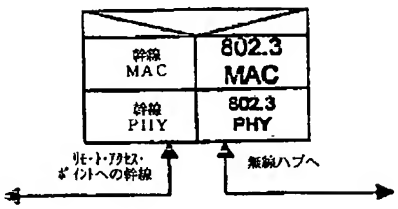
【図4】



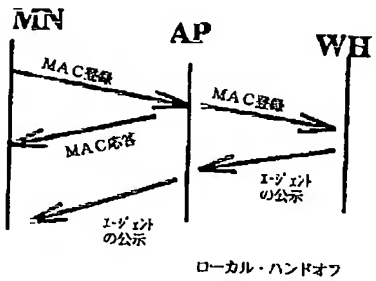
【図7】



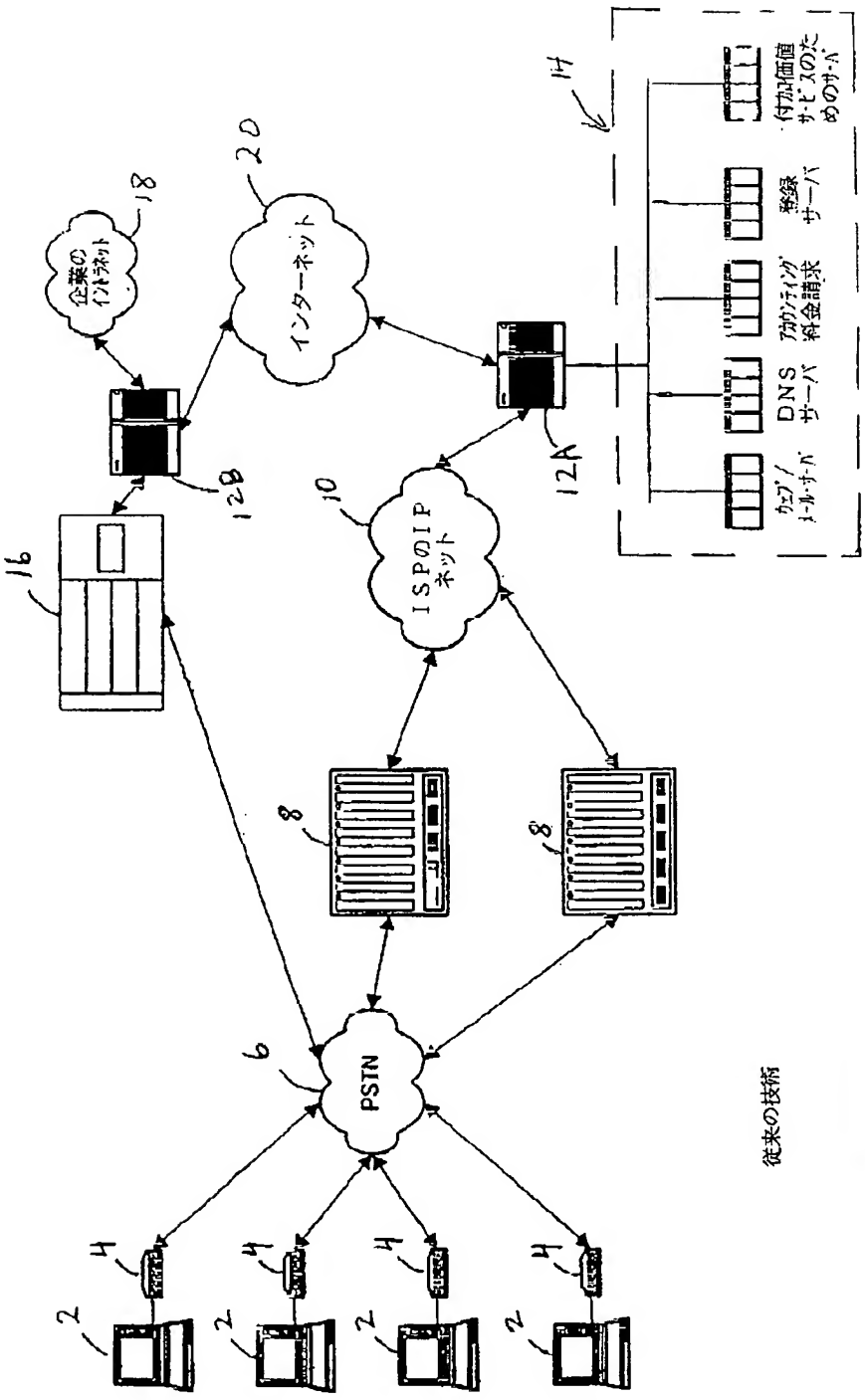
【図8】



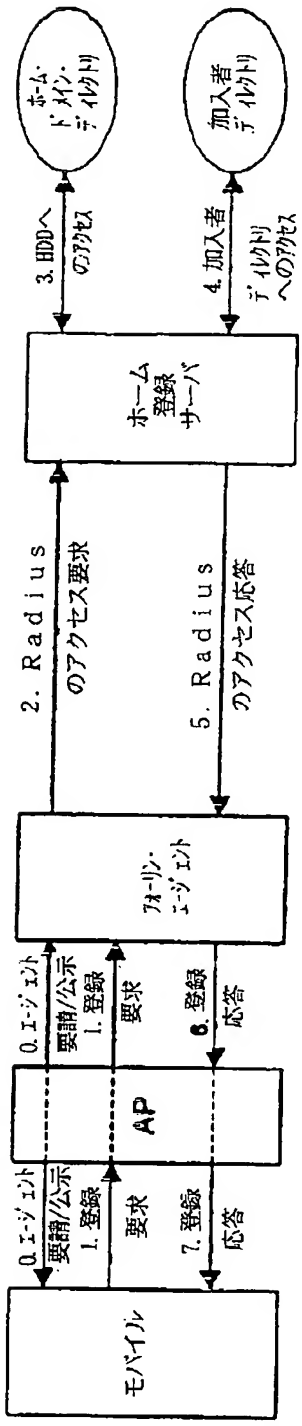
【図29】



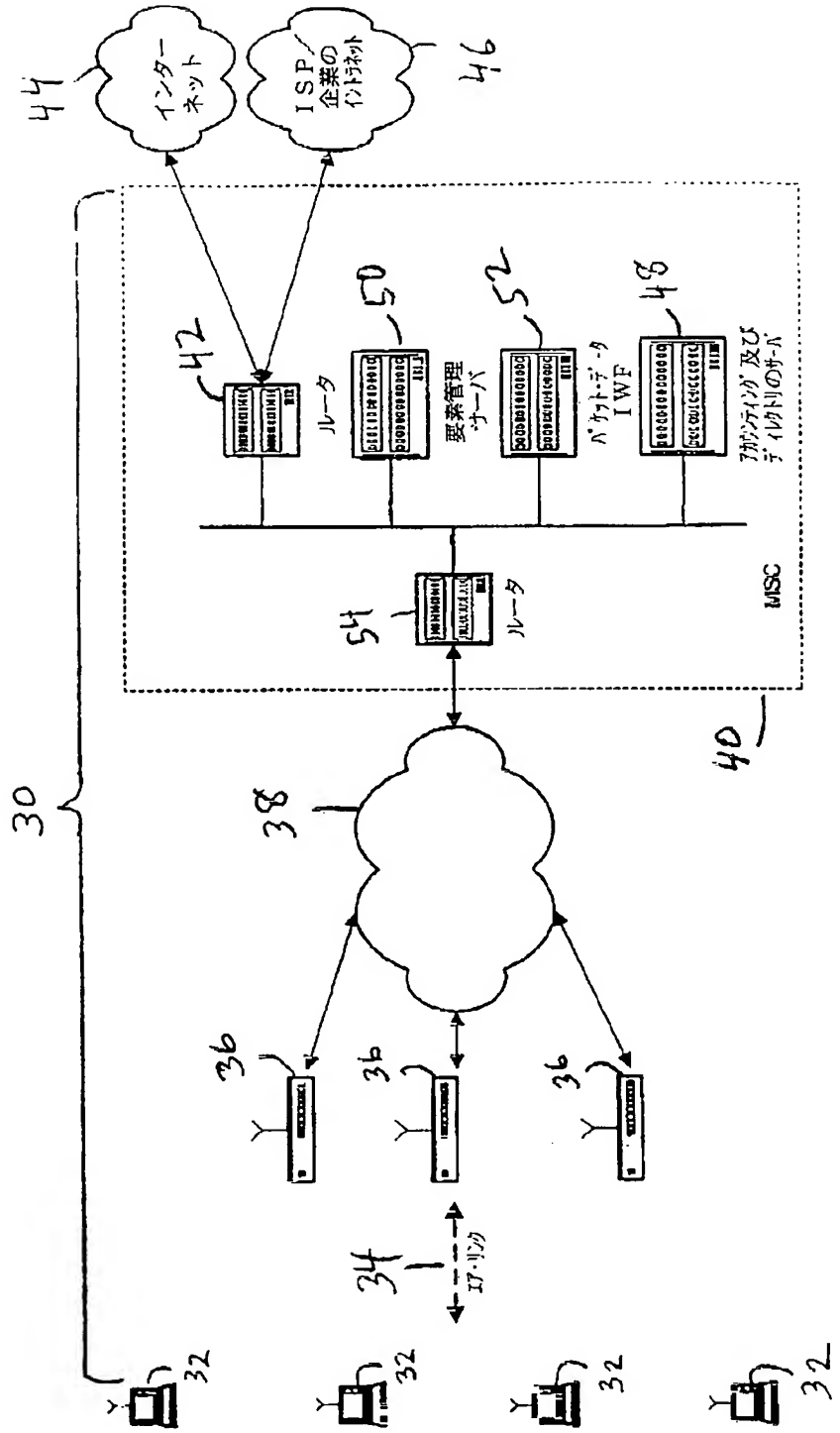
【図1】


企業のイントラネット
18
インターネット
20
14
12B
12A
16
10
ISPのIPネット
8
8
PSTN
6
4
4
4
4
2
2
2
2
ウェブ/メール・サーバ
DNS サーバ
アカウンティング/料金請求
登録 サーバ
付加価値サービスのためのサーバ
従来の技術

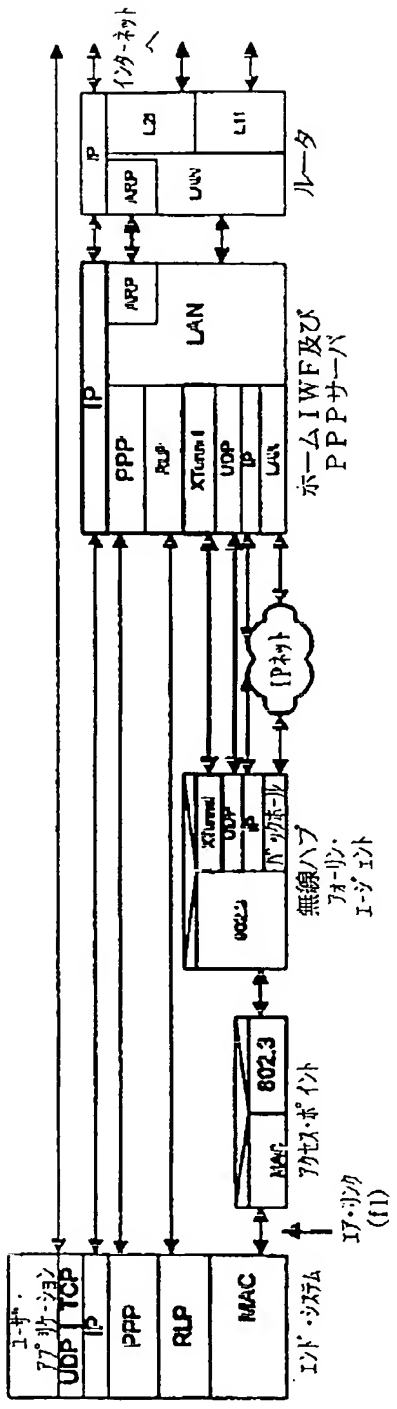
【図15】


ホーム無線サービス・プロバイダ
ホーム・ドメイン・データベース
加入者データベース
3. HDDへのアクセス
4. 加入者データへのアクセス
ホーム登録サーバ
2. Radiusのアクセス要求
5. Radiusのアクセス応答
フォーリン・エージェント
0. エージェント要請/公示
1. 登録要求
6. 登録応答
AP
0. エージェント要請/公示
1. 登録要求
7. 登録応答
モバイル

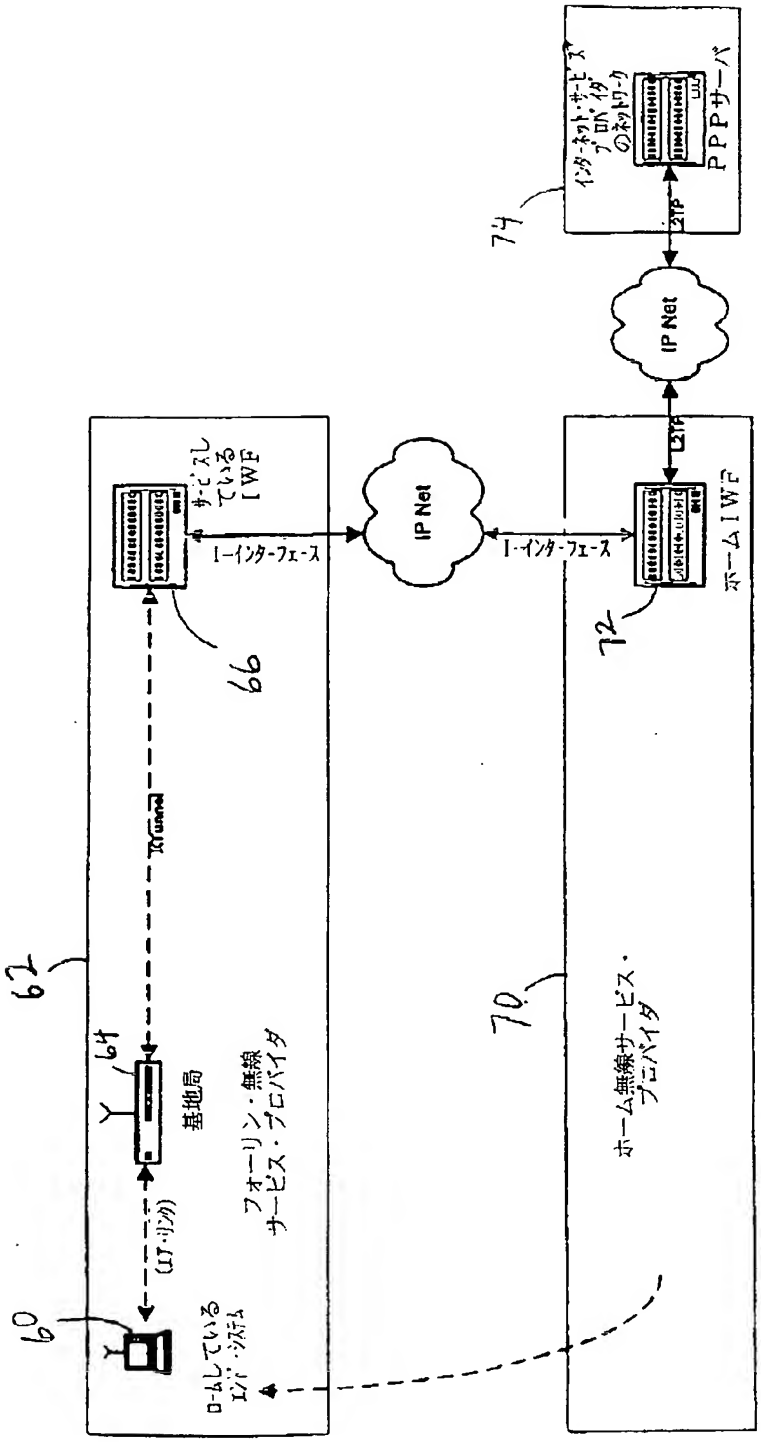
【図2】


インター-ネット
ISP/企業のイントラネット
ルータ
要素管理サーバ
パケット・データIWF
アカウンティング及びディレクトリのサーバ
ルータ
MSC
エア・リンク
エンド・システム

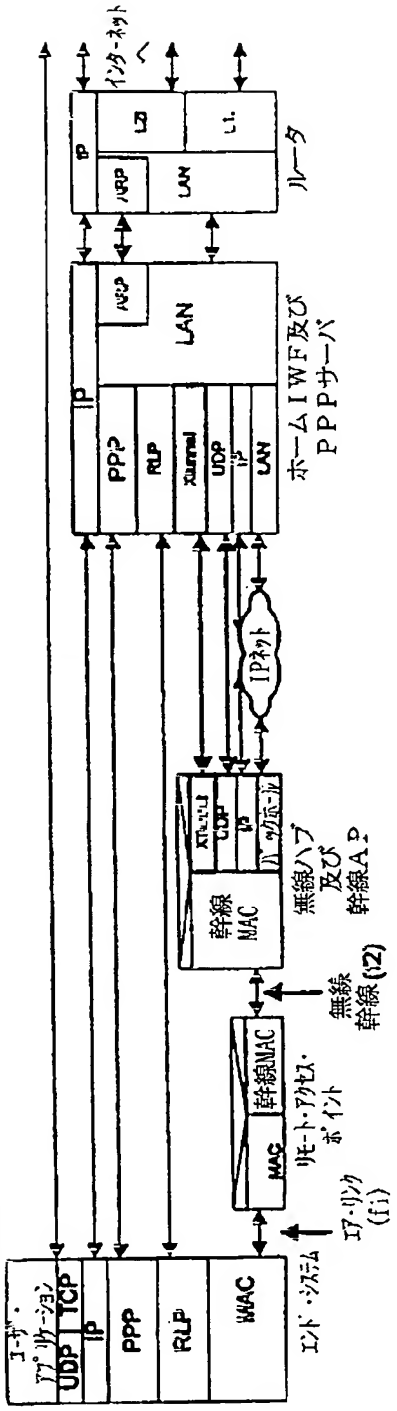
【図17】


インター-ネットへ
ルータ
ホームIWF及びPPPサーバ
IP
ARP
LAN
PPP
RLP
XTunnel
UDP
LAP
IPネット
無線ハブ
フォーリン・エージェント
802.3
MAC
アクセス・ポイント
エア・リンク
(11)
エンド・システム
MAC
RLP
PPP
UDP
TCP

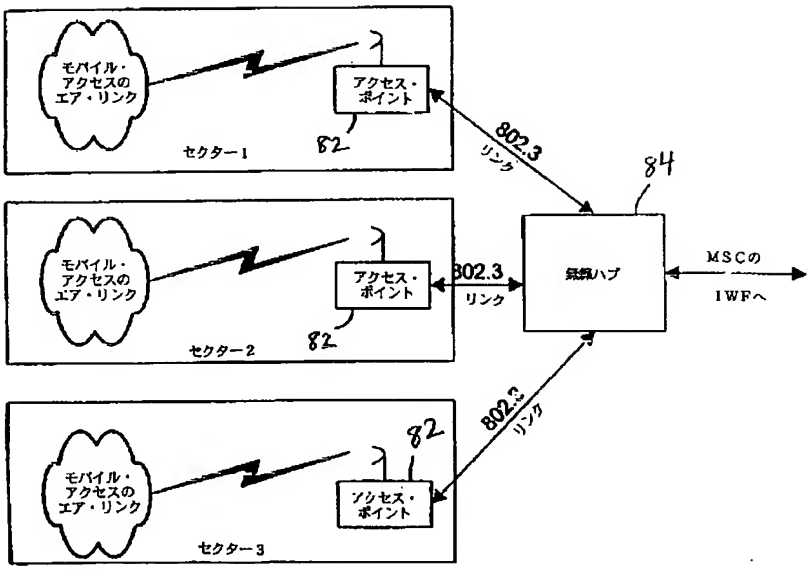
【図3】


IP Net
IP Net
PPPサーバ
ホームIWF
基地局
フォーリン・無線
サービス・プロバイダ
ホーム無線サービス・
プロバイダ
62
64
66
70
72
74

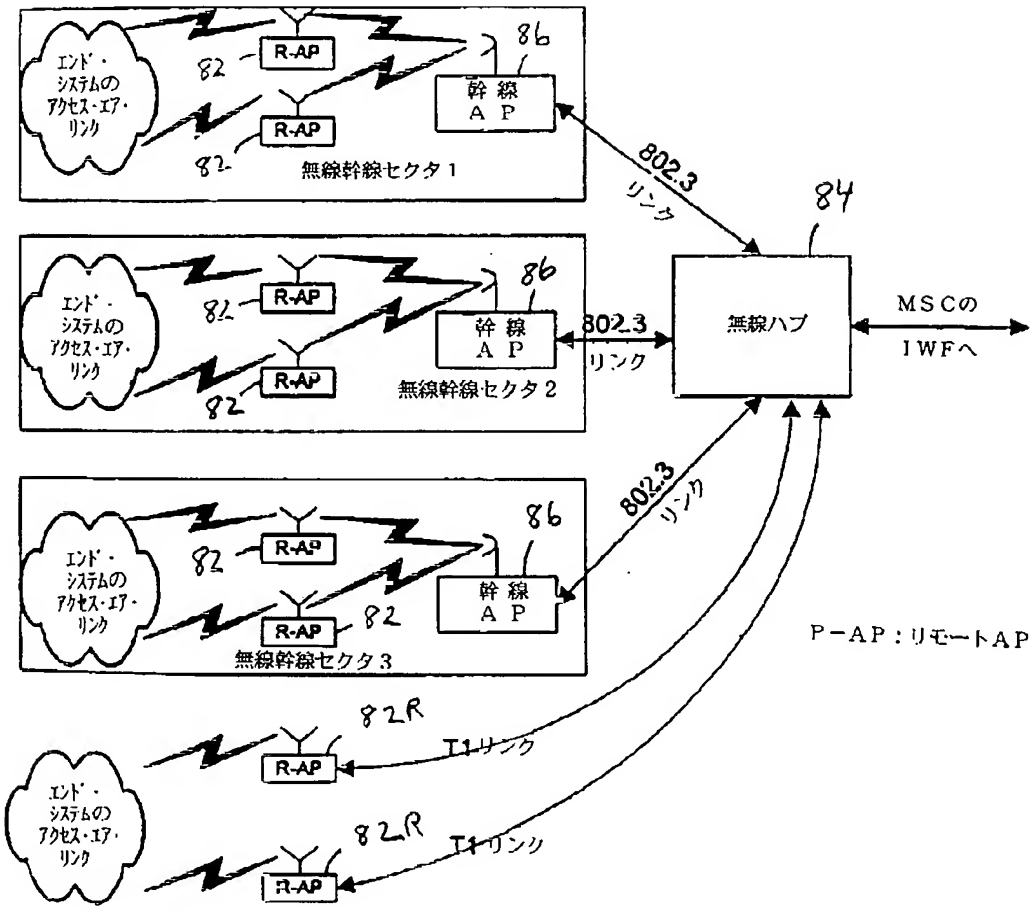
【図18】


インターネットへ
ルータ
LAN
PPP
RLP
WAC
IPネット
幹線MAC
無線ハブ及び幹線AP
無線幹線(12)
エア・リンク(11)
エンド・システム

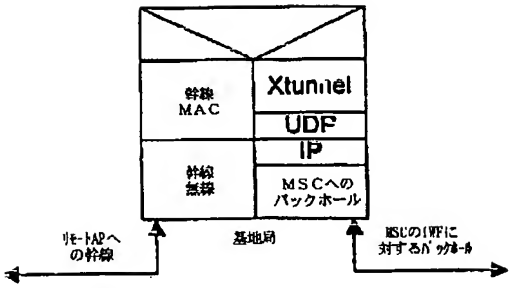
【図５】


モバイル・
アクセスの
エア・リンク
アクセス・
ポイント
82
セクター1
802.3
リンク
84
無線ハブ
MSCの
IWFへ
セクター2
セクター3

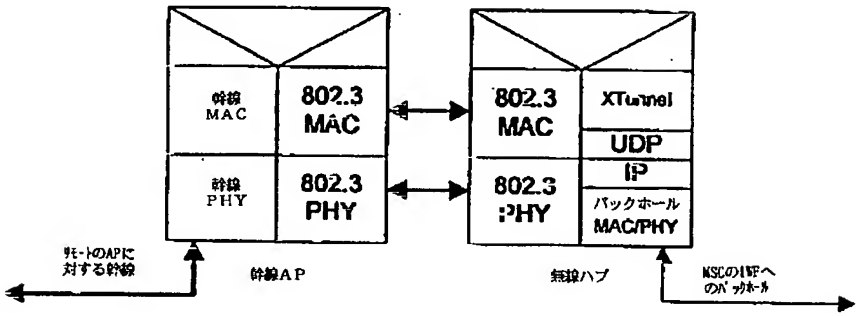
【図６】


エンド・
システムの
アクセス・エア・
リンク
R-AP
82
86
幹線
ＡＰ
無線幹線セクタ１
802.3
リンク
84
無線ハブ
MSCの
IWFへ
無線幹線セクタ２
無線幹線セクタ３
P－AP：リモートAP
82R
T1リンク

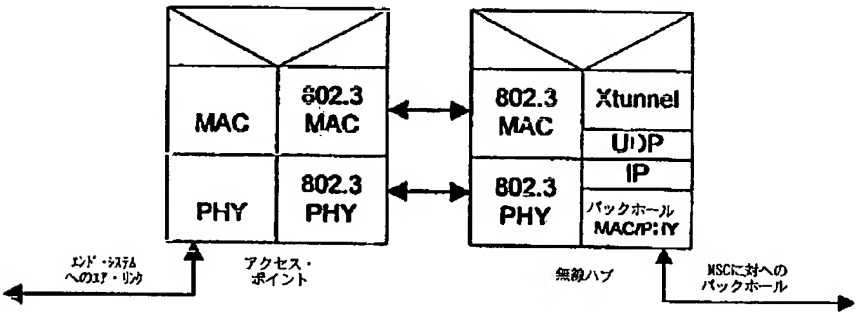
【図９】



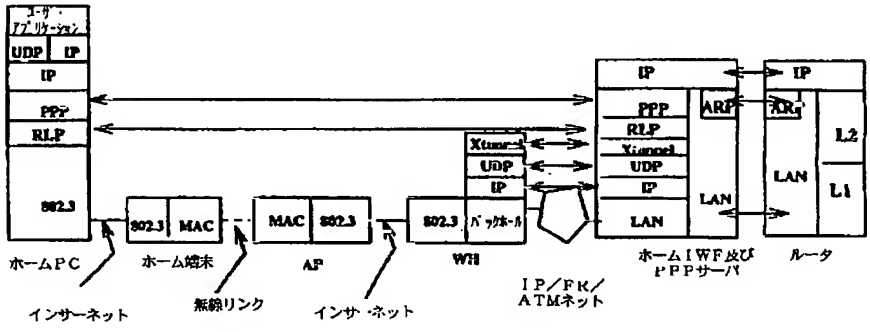
【図１０】



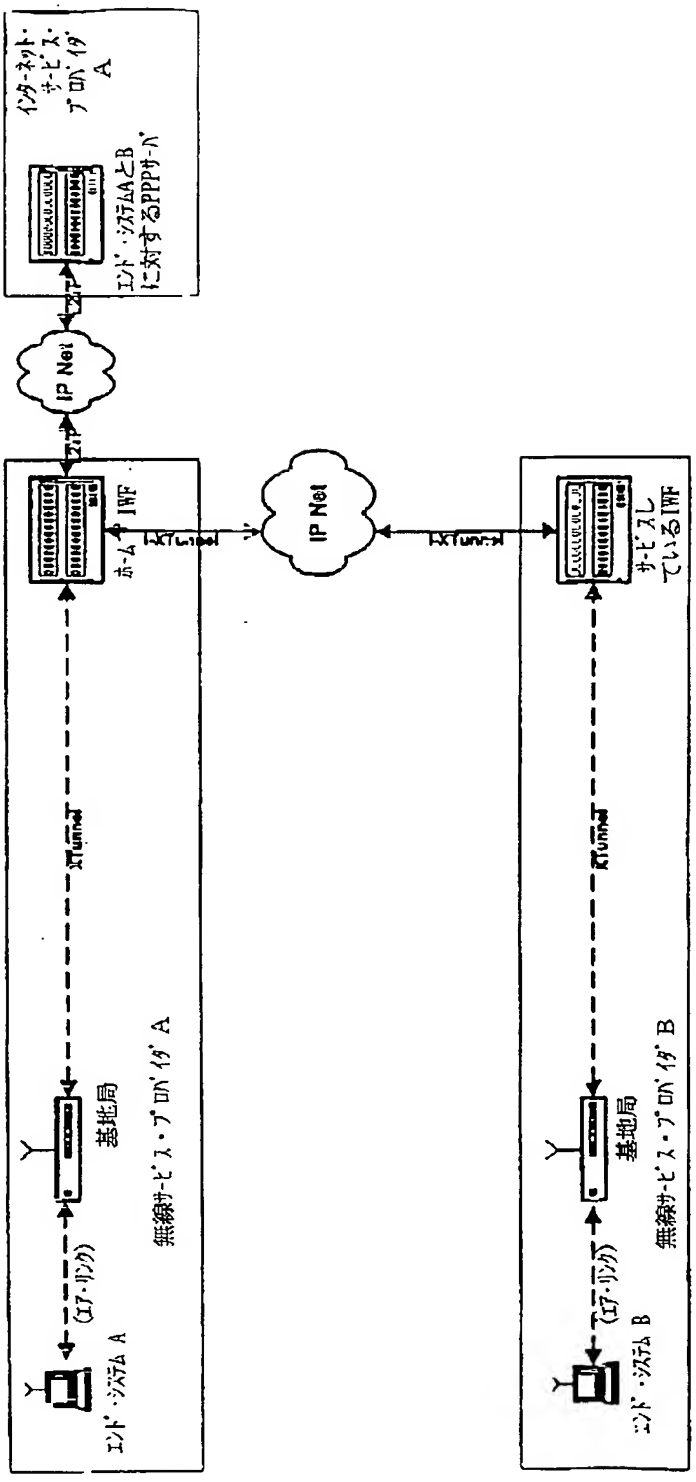
【図１１】



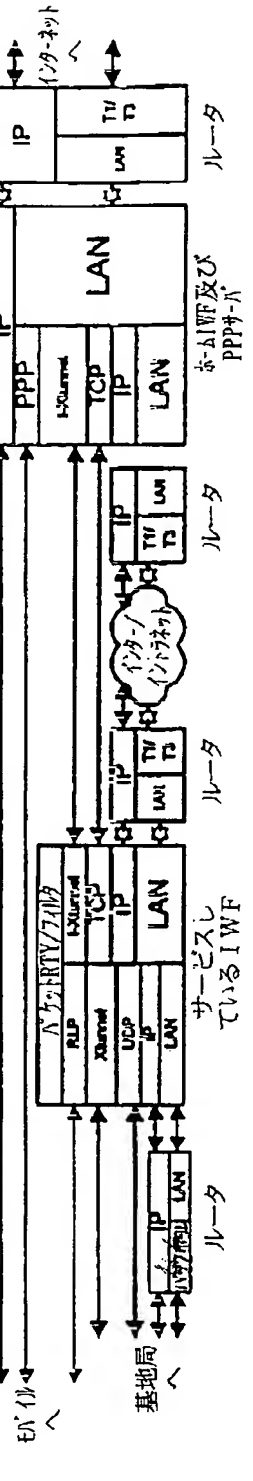
【図２５】



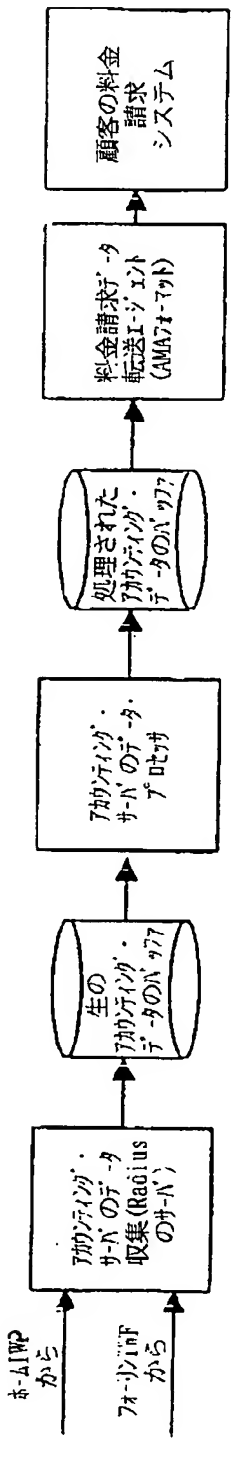
【図12】


インターネット・サービス・プロバイダA
エンド・システムAとBに対するPPPサーバ
IP Net
IWF
ホーム
Tunnel
IP Net
サービスしているIWF
基地局
無線サービス・プロバイダB
エア・リンク
エンド・システム A
エンド・システム B

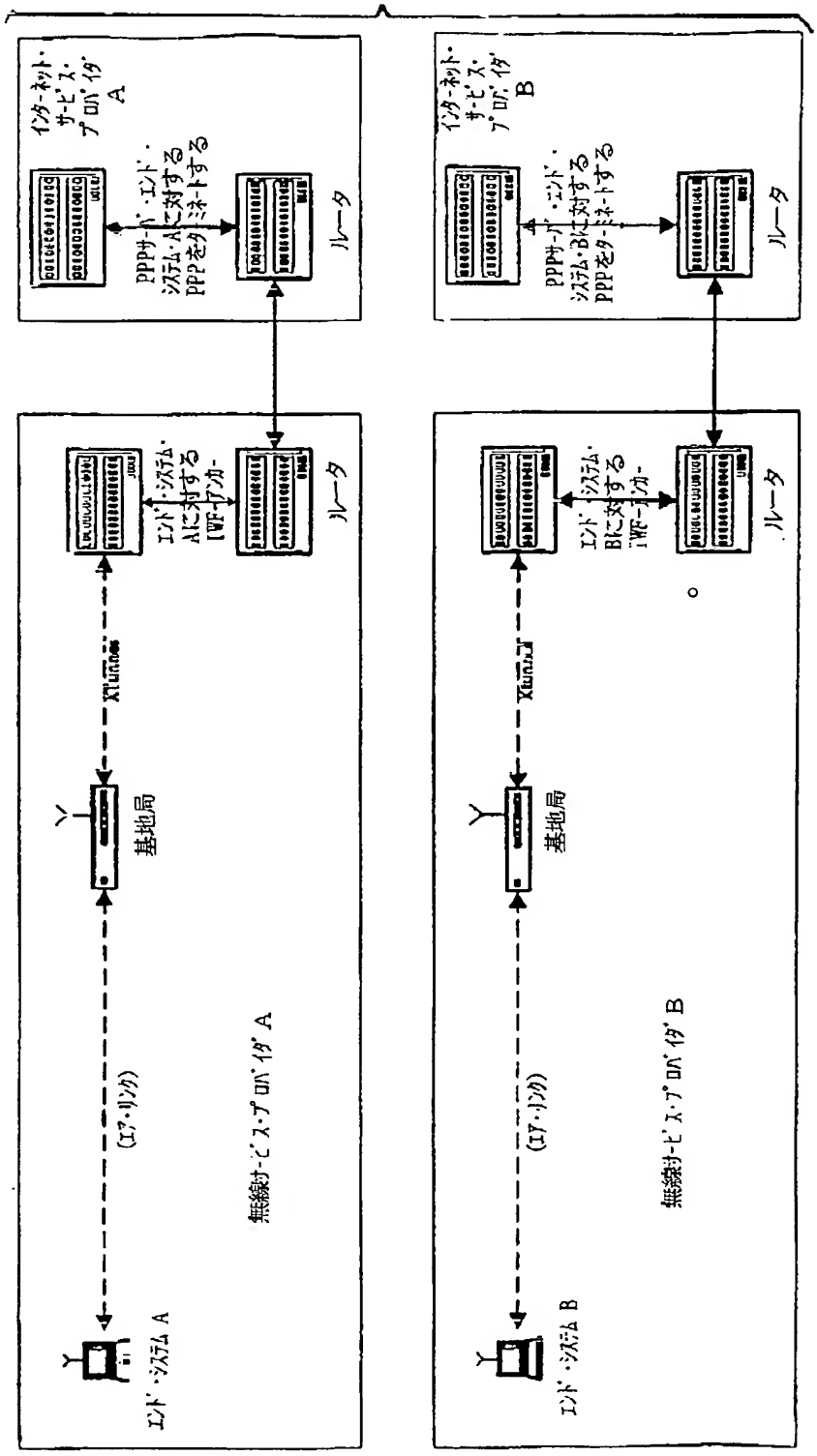
【図19】


インターネットへ
IP
TCP/UDP
LAN
ルータ
PPP
L2tunnel
ホームIWF及びPPPサーバ
パケットRTV/フォワ
RLP
UDP
サービスしているIWF
インターネット
基地局へ
モバイルへ

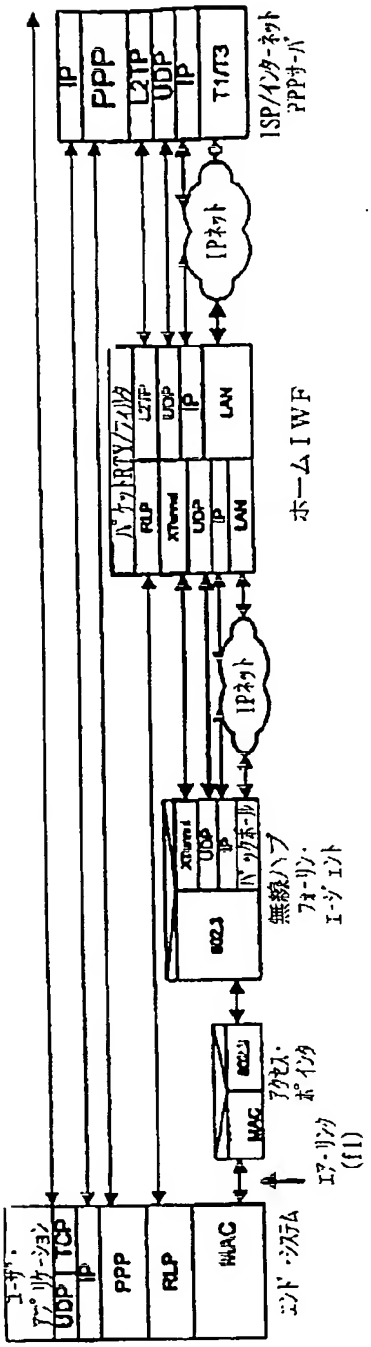
【図22】


顧客の料金請求システム
料金請求データ転送エージェント(AMAフォーマット)
処理されたアカウンティング・データのバッファ
アカウンティング・サーバのデータ・プロセサ
生のアカウンティング・データのバッファ
アカウンティング・サーバのデータ収集(Radius のサーバ)
ホームIWFから
フォーリンFから

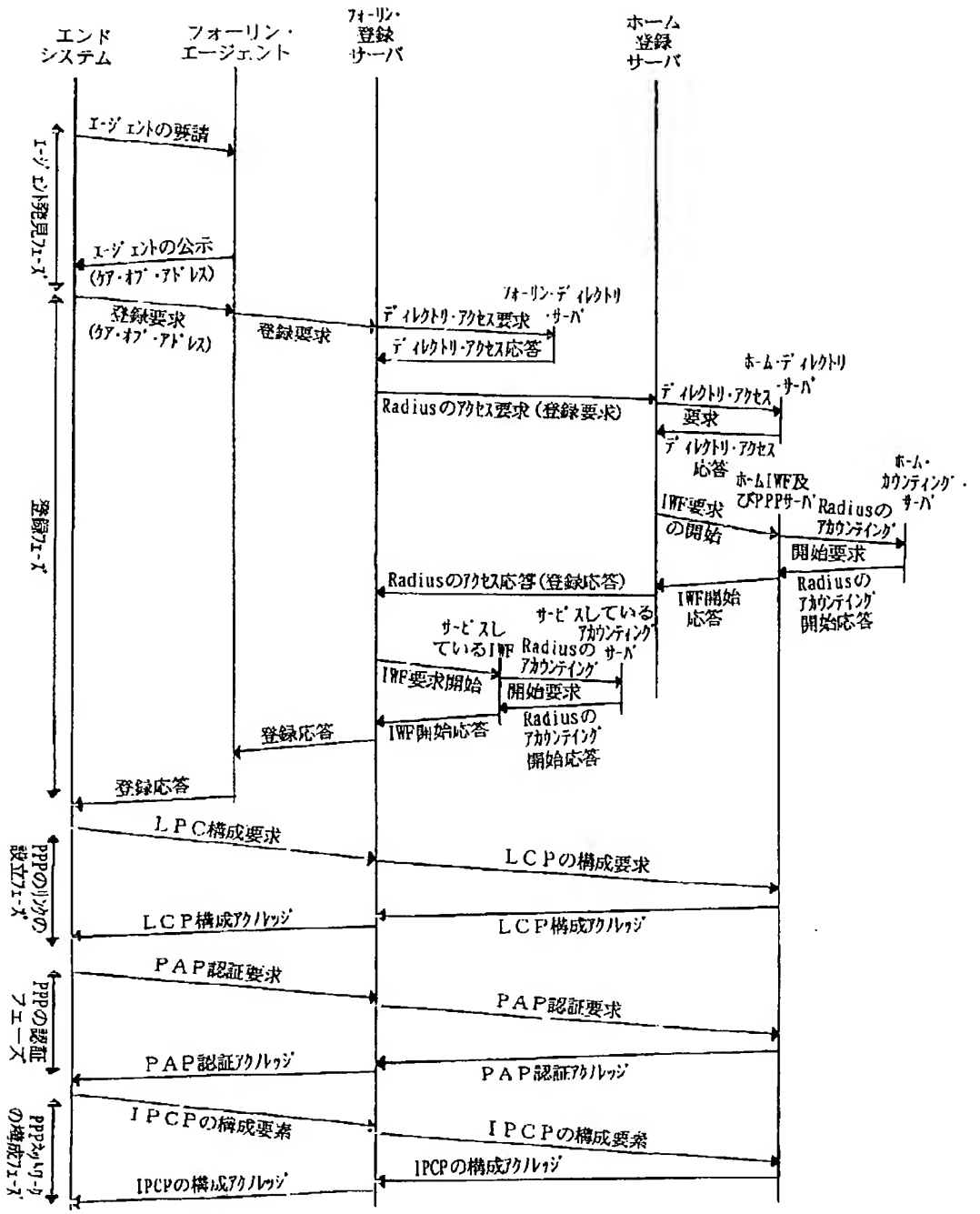
【図13】


インターネット・サービス・プロバイダ A
PPPサーバ・エンド・システムAに対するPPPをターミネートする
ルータ
エンド・システムAに対するIWFエンティティ
基地局
(エア・リンク)
エンド・システム A
無線サービス・プロバイダ A
インターネット・サービス・プロバイダ B
PPPサーバ・エンド・システムBに対するPPPをターミネートする
エンド・システムBに対するIWFエンティティ
エンド・システム B
無線サービス・プロバイダ B

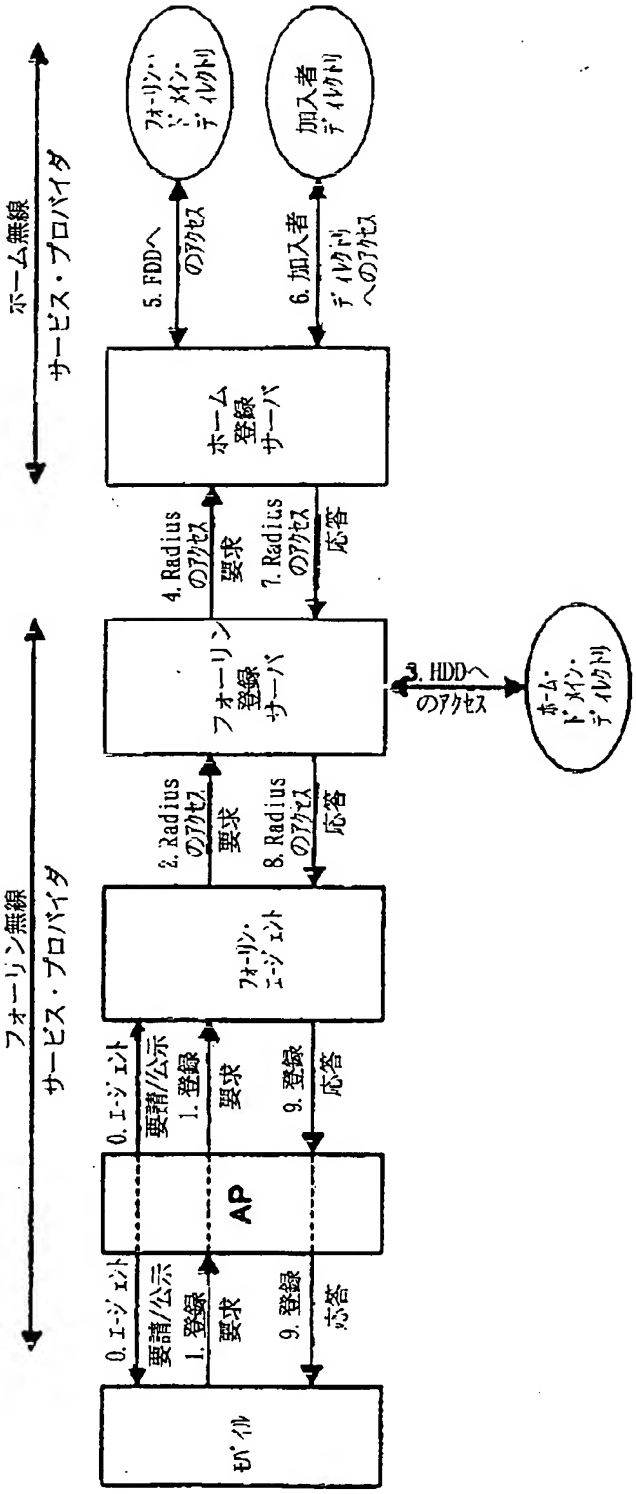
【図20】


IP
PPP
L2TP
UDP
IP
T1/E1
ISP/インターネット PPPサーバ
IPネット
パケットRTVプロトコル
LAN
IPネット
無線ハブ アクセス・ポイント
エア・リンク (f1)
エンド・システム
ホームIWF

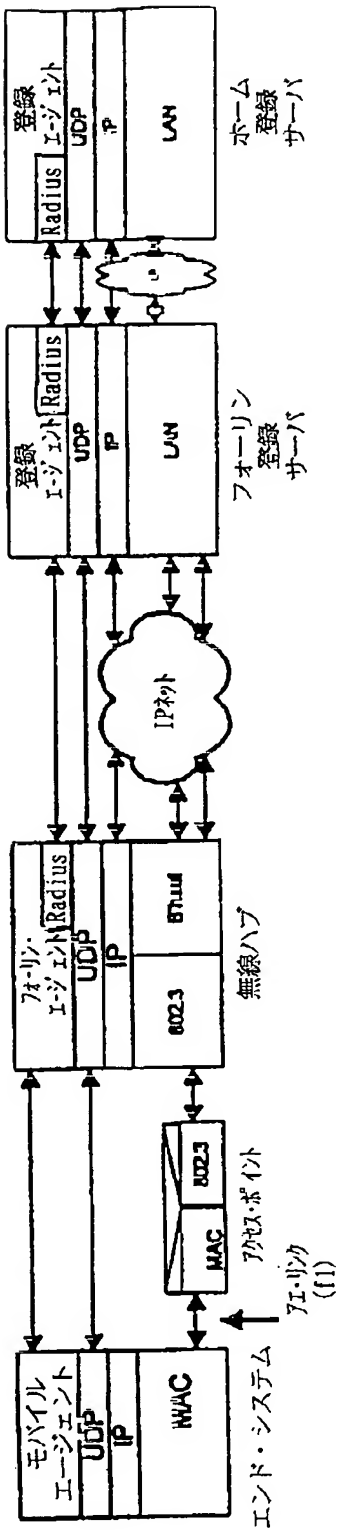
【図１４】


エンド
システム
フォーリン・
エージェント
フォーリン・
登録
サーバ
ホーム
登録
サーバ
エージェント発見フェーズ
エージェントの要請
エージェントの公示
(ケア・オブ・アドレス)
登録要求
(ケア・オブ・アドレス)
登録要求
フォーリン・ディレクトリ
・サーバ
ディレクトリ・アクセス要求
ディレクトリ・アクセス応答
ホーム・ディレクトリ
・サーバ
ディレクトリ・アクセス
要求
ディレクトリ・アクセス
応答
Radiusのアクセス要求(登録要求)
登録フェーズ
ホームIWF及
びPPPサーバ
ホーム・
カウンティング・
サーバ
IWF要求
の開始
Radiusの
アカウンティング
開始要求
Radiusのアクセス応答(登録応答)
IWF開始
応答
Radiusの
アカウンティング
開始応答
サービスしている
アカウンティング
サーバ
サービスしている
IWF
IWF要求開始
Radiusの
アカウンティング
開始要求
Radiusの
アカウンティング
開始応答
IWF開始応答
登録応答
登録応答
PPPのリンクの
設立フェーズ
LPC構成要求
LCPの構成要求
LCP構成アクノレッジ
LCP構成アクノレッジ
PPPの認証
フェーズ
PAP認証要求
PAP認証要求
PAP認証アクノレッジ
PAP認証アクノレッジ
PPPネットワーク
の構成フェーズ
IPCPの構成要素
IPCPの構成要素
IPCPの構成アクノレッジ
IPCPの構成アクノレッジ

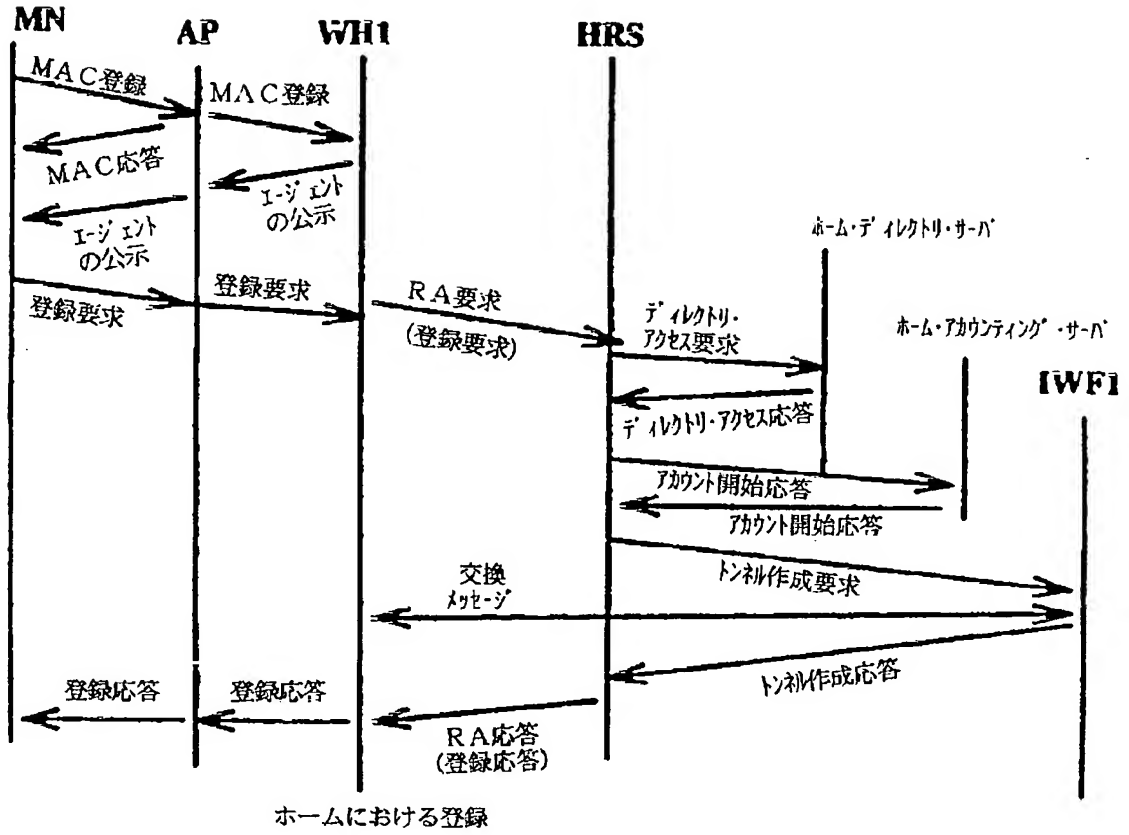
【図16】


ホーム無線
サービス・プロバイダ
フォーリン無線
サービス・プロバイダ
フォーリン・ドメイン・ディレクトリ
加入者ディレクトリ
5. FDDへのアクセス
6. 加入者ディレクトリへのアクセス
ホーム登録サーバ
4. Radiusのアクセス
要求
7. Radiusのアクセス
応答
フォーリン登録サーバ
3. HDDへのアクセス
ホーム・ドメイン・ディレクトリ
2. Radiusのアクセス
要求
8. Radiusのアクセス
応答
フォーリン・エージェント
0. エージェント要請/公示
1. 登録要求
9. 登録応答
AP
0. エージェント要請/公示
1. 登録要求
9. 登録応答
モバイル

【図21】

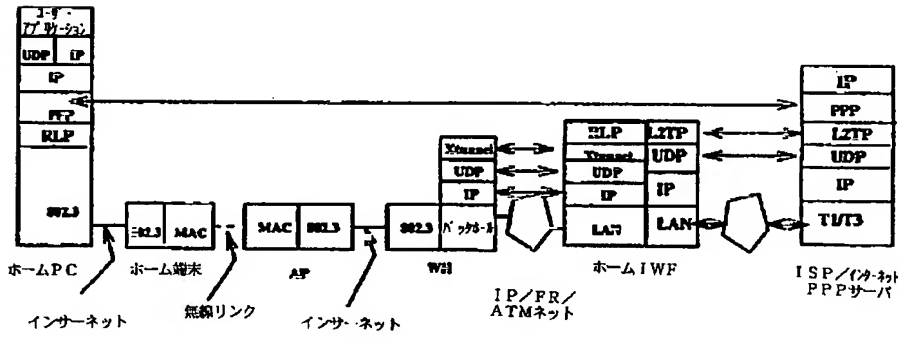

登録エージェント
Radius
UDP
IP
LAN
ホーム登録サーバ
フォーリン登録サーバ
IPネットワーク
フォーリン・エージェント
802.3
Ethernet
無線ハブ
MAC
802.3
アクセス・ポイント
フォーリンク(f1)
モバイルエージェント
NWAC
エンド・システム

【図２３】

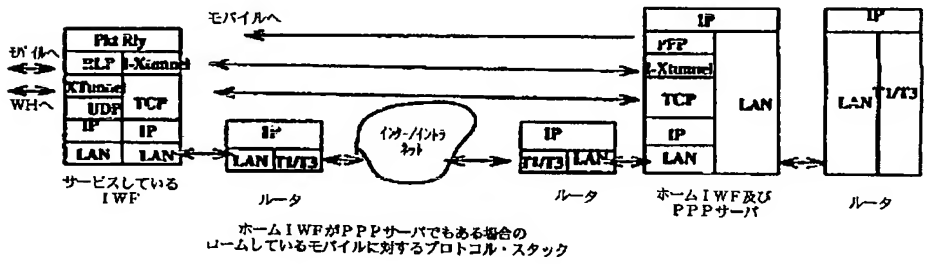


ホームにおける登録

【図２６】

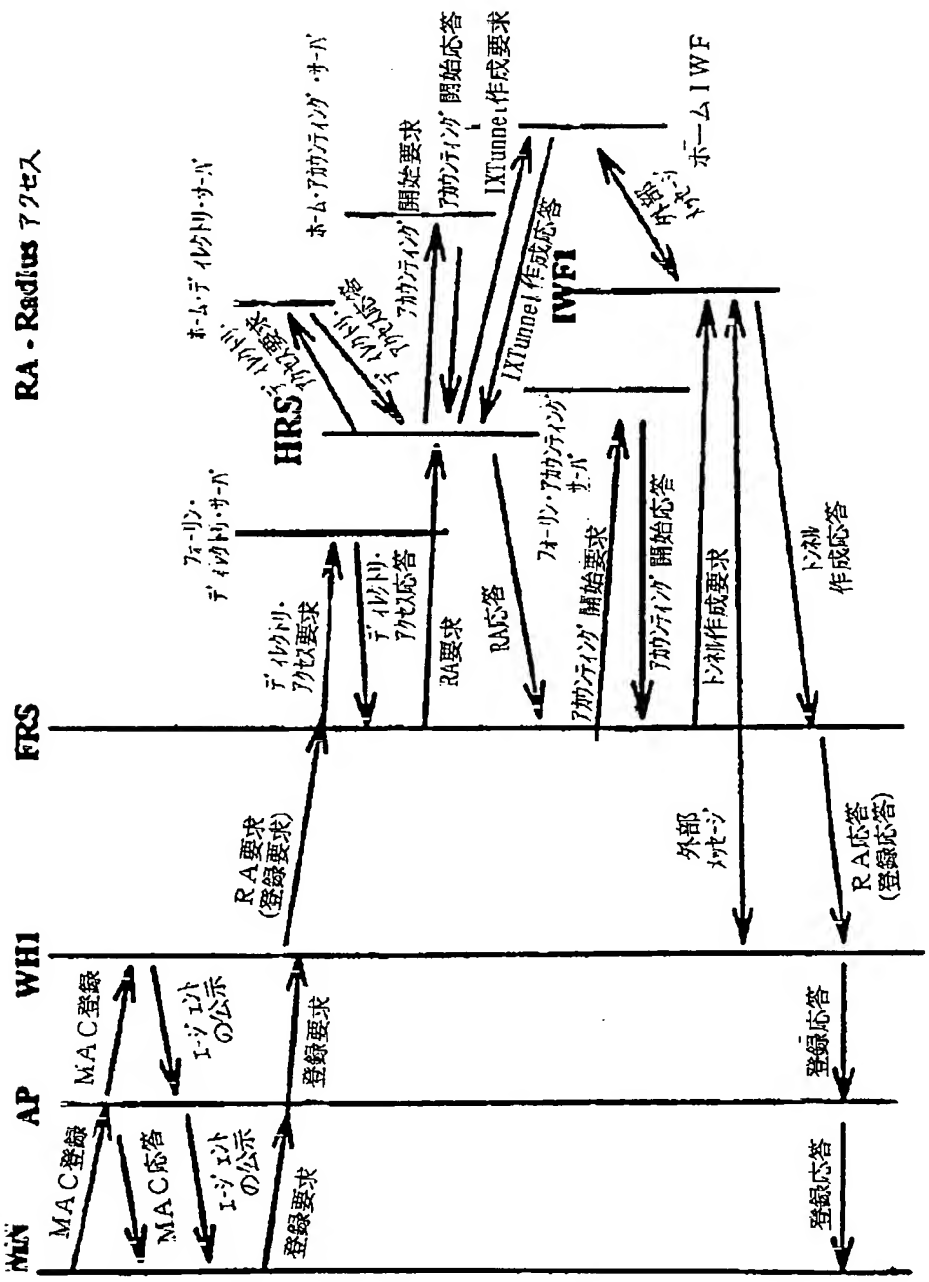


【図２７】

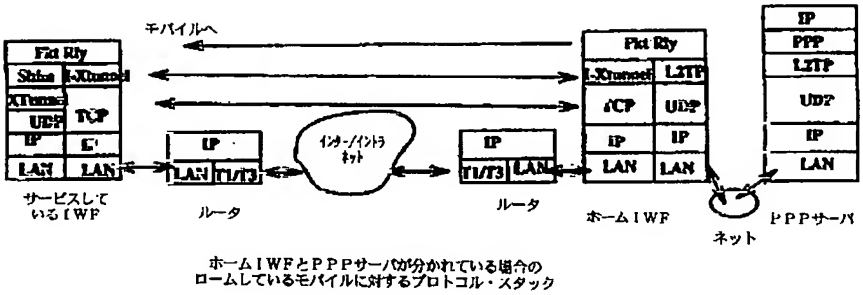


ホームＩＷＦがＰＰＰサーバでもある場合の
ローミングしているモバイルに対するプロトコル・スタック

【図２４】

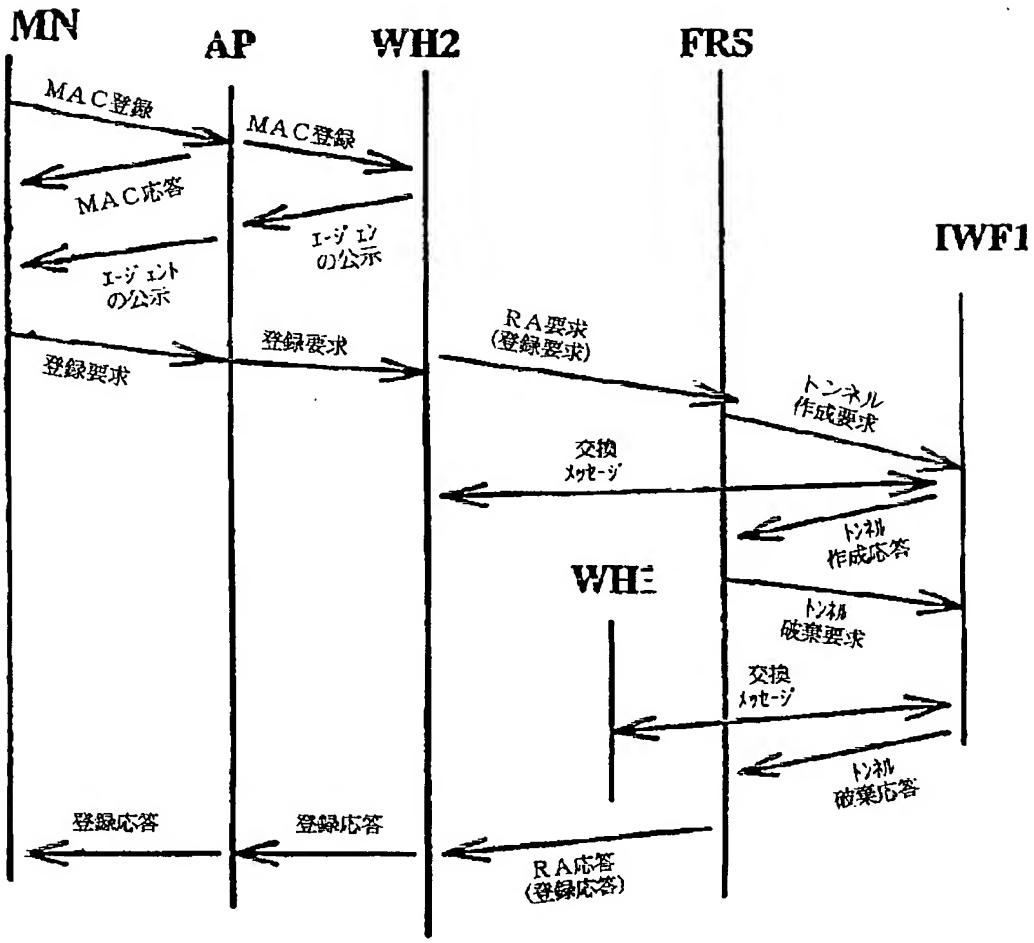

RA・Radius アクセス
MN
AP
WH1
FRS
HRS
IWF1
MAC登録
MAC応答
エージェントの公示
登録要求
RA要求（登録要求）
RA応答（登録応答）
登録応答
ディレクトリ・アクセス要求
ディレクトリ・アクセス応答
RA要求
RA応答
フォーリン・アカンティング・開始要求
アカンティング・開始応答
トンネル作成要求
トンネル作成応答
外部メッセージ
IXTunnel作成要求
IXTunnel作成応答
ホーム・アカンティング・開始要求
ホーム・アカンティング・開始応答
ホーム IWF

【図28】



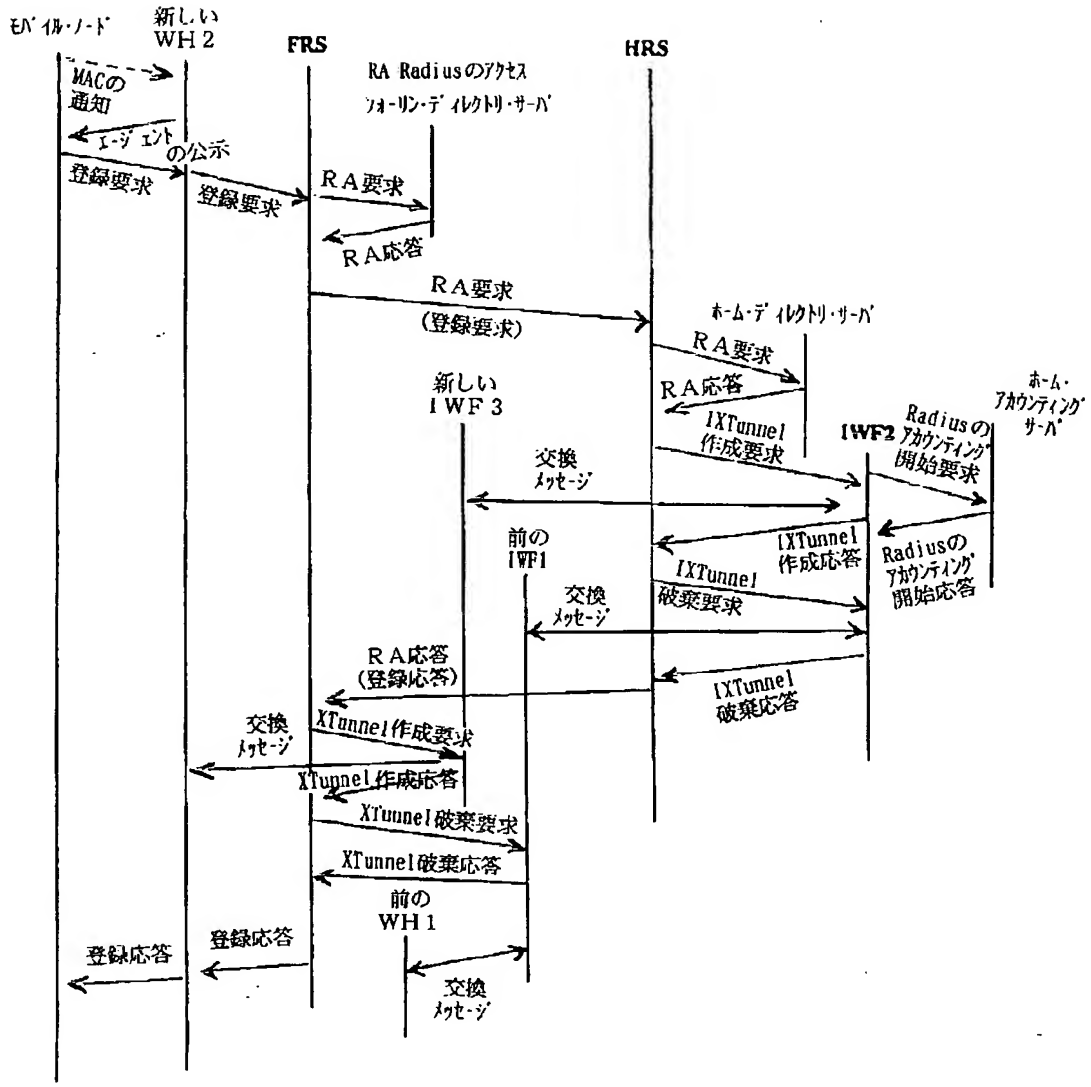
ホームIWFとPPPサーバが分かれている場合の
ロームしているモバイルに対するプロトコル・スタック

【図30】

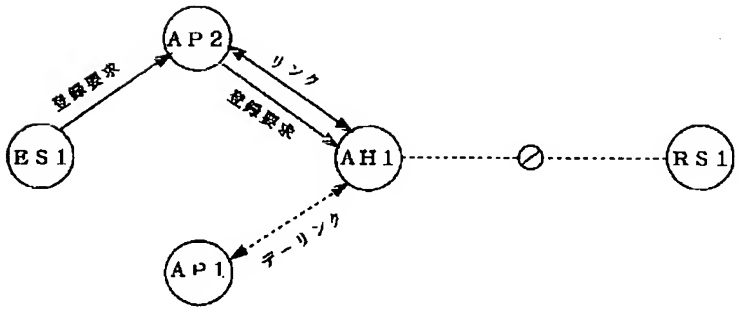


マイクロ・モビリティ

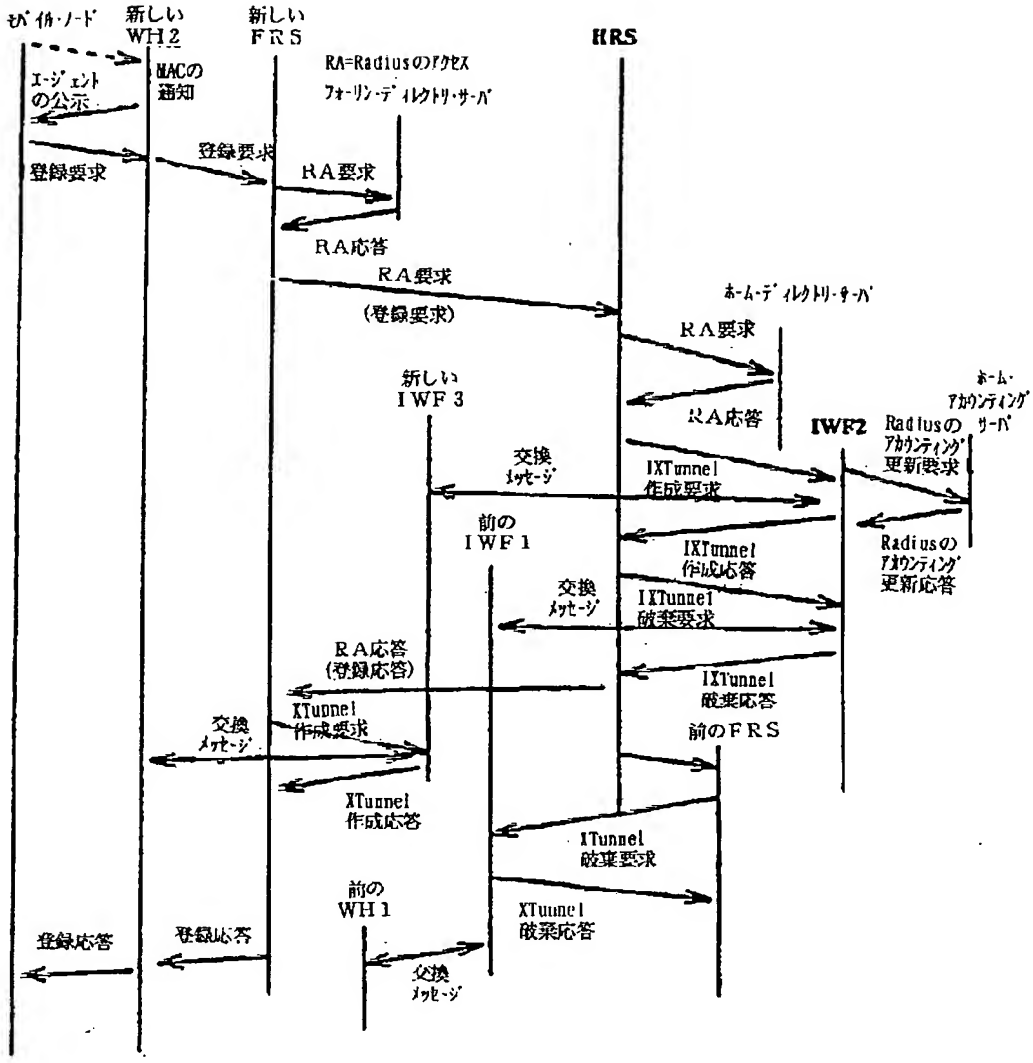
【図３１】


ﾓﾊﾞｲﾙ･ﾉｰﾄﾞ
新しい WH２
FRS
RA Radiusのｱｸｾｽ ｿｫｰﾘﾝ･ﾃﾞｨﾚｸﾄﾘ･ｻｰﾊﾞ
HRS
MACの通知
ｴｰｼﾞｪﾝﾄの公示
登録要求
登録要求
RA要求
RA応答
RA要求 (登録要求)
ﾎｰﾑ･ﾃﾞｨﾚｸﾄﾘ･ｻｰﾊﾞ
RA要求
RA応答
新しい IWF３
IXTunnel 作成要求
IWF2
Radiusの ｱｶｳﾝﾃｨﾝｸﾞ 開始要求
ﾎｰﾑ･ ｱｶｳﾝﾃｨﾝｸﾞ ｻｰﾊﾞ
交換 ﾒｯｾｰｼﾞ
前の IWF1
IXTunnel 作成応答
Radiusの ｱｶｳﾝﾃｨﾝｸﾞ 開始応答
IXTunnel 破棄要求
交換 ﾒｯｾｰｼﾞ
RA応答 (登録応答)
IXTunnel 破棄応答
交換 ﾒｯｾｰｼﾞ
XTunnel作成要求
XTunnel作成応答
XTunnel破棄要求
XTunnel破棄応答
前の WH１
登録応答
登録応答
交換 ﾒｯｾｰｼﾞ

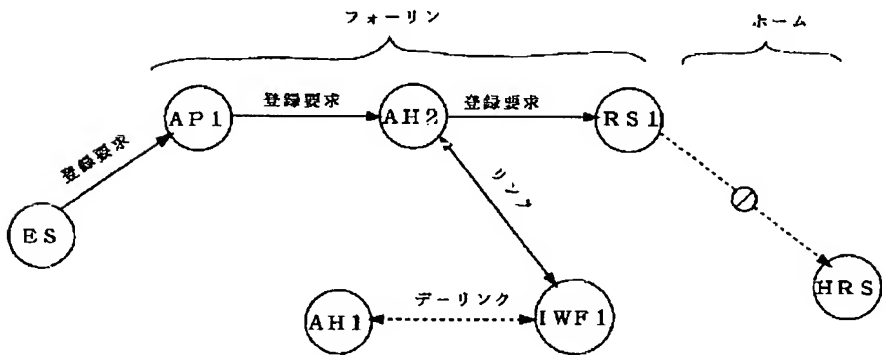
【図３４】


AP２
リンク
登録要求
登録要求
ES１
AH１
RS１
ﾘｰﾘﾝｸ
AP１

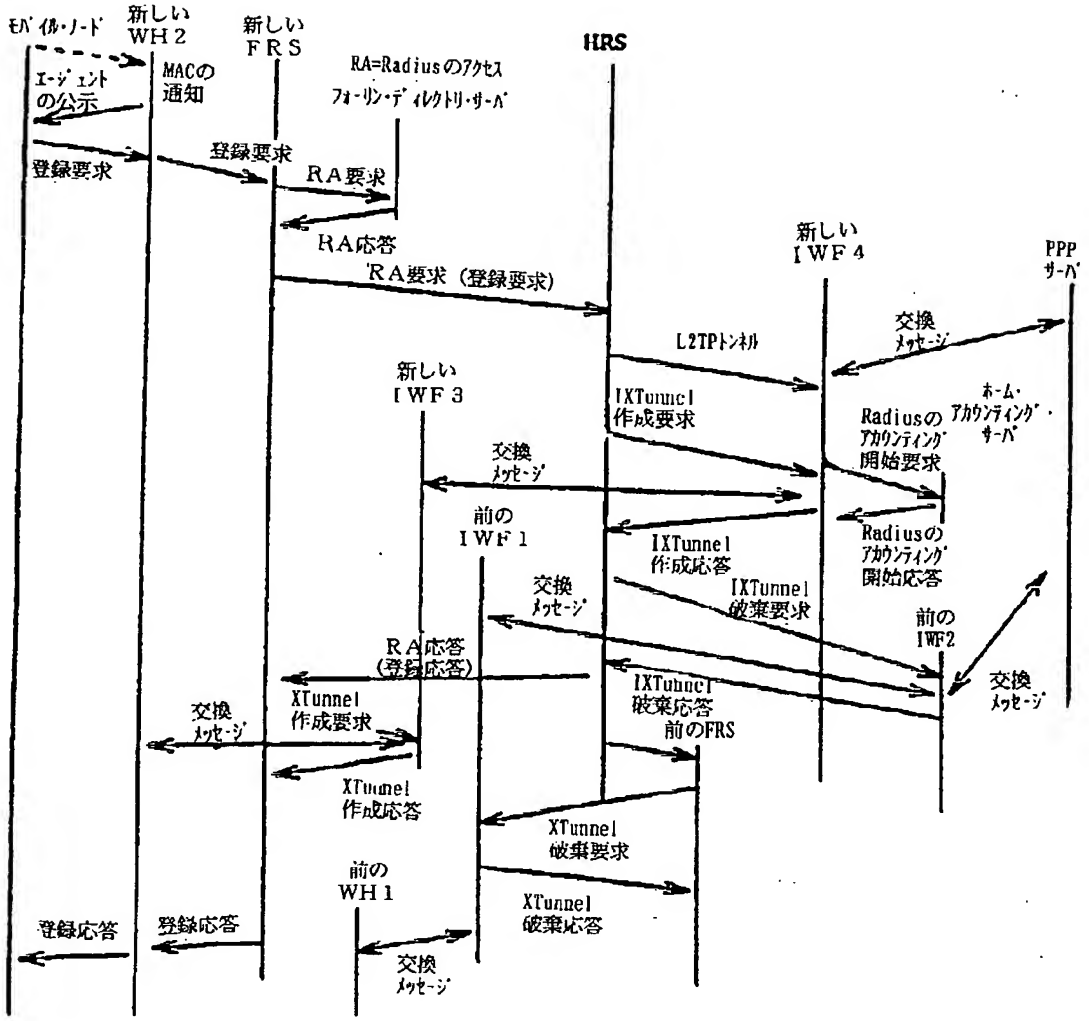
【図３２】


新しい
WH2
新しい
FRS
HRS
RA=Radiusのアクセスフォーリンディレクトリサーバ
MACの通知
エージェントの公示
登録要求
登録要求
RA要求
RA応答
RA要求
(登録要求)
ホームディレクトリサーバ
RA要求
RA応答
新しい
IWF3
IWF2
Radiusのアカウンティング更新要求
ホームアカウンティングサーバ
交換メッセージ
IXTunnel作成要求
前の
IWF1
IXTunnel作成応答
Radiusのアカウンティング更新応答
交換メッセージ
IXTunnel破棄要求
RA応答
(登録応答)
IXTunnel破棄応答
XTunnel作成要求
交換メッセージ
前のFRS
XTunnel作成応答
XTunnel破棄要求
前の
WH1
XTunnel破棄応答
登録応答
登録応答
交換メッセージ

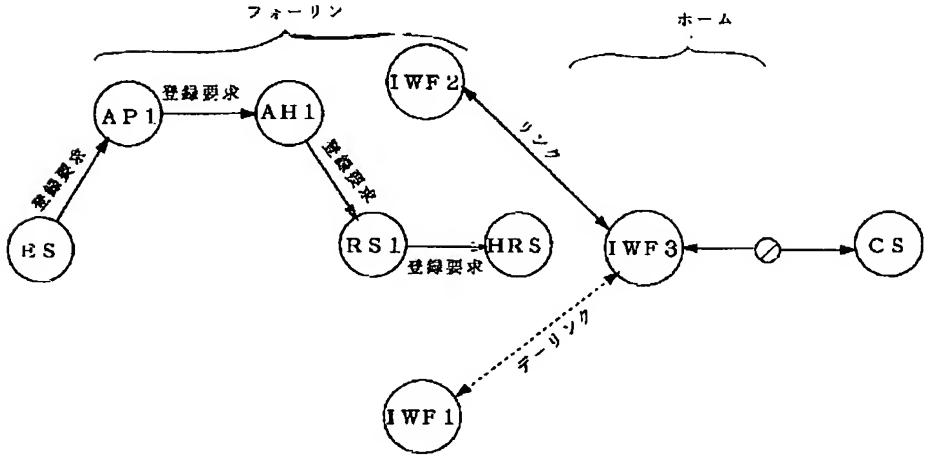
【図３５】


フォーリン
ホーム
AP1
登録要求
AH2
登録要求
RS1
登録要求
ES
リンク
HRS
AH1
データリンク
IWF1

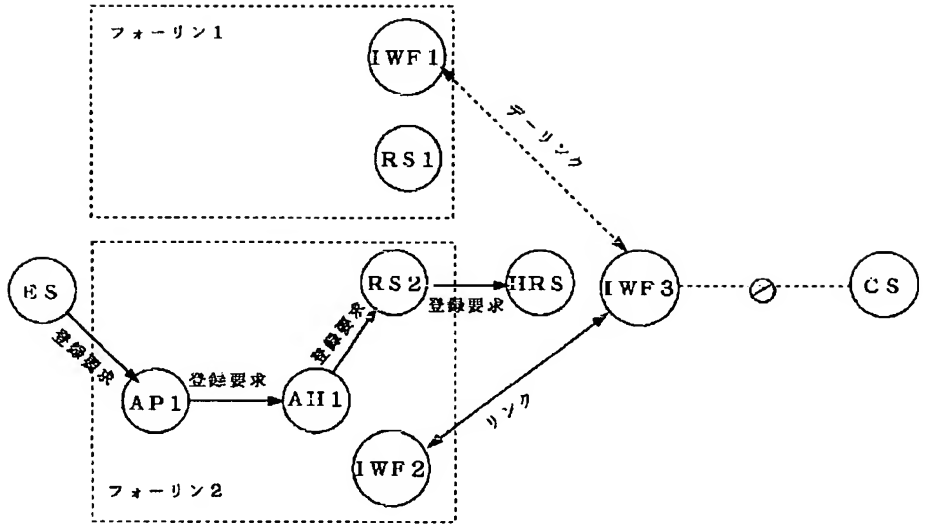
【図３３】


モバイル・ノード
新しい WH２
新しい FRS
HRS
RA=Radiusのアクセス フォーリン・ディレクトリ・サーバ
エージェントの公示
MACの通知
登録要求
登録要求
RA要求
RA応答
RA要求（登録要求）
新しい IWF４
PPP サーバ
交換メッセージ
L2TPトンネル
新しい IWF３
IXTunnel 作成要求
Radiusの アカウンティング 開始要求
ホーム・アカウンティング・サーバ
交換メッセージ
前の IWF１
IXTunnel 作成応答
Radiusの アカウンティング 開始応答
交換メッセージ
IXTunnel 破棄要求
前の IWF２
RA応答（登録応答）
IXTunnel 破棄応答
前のFRS
交換メッセージ
XTunnel 作成要求
交換メッセージ
XTunnel 作成応答
XTunnel 破棄要求
前の WH１
XTunnel 破棄応答
登録応答
登録応答
交換メッセージ

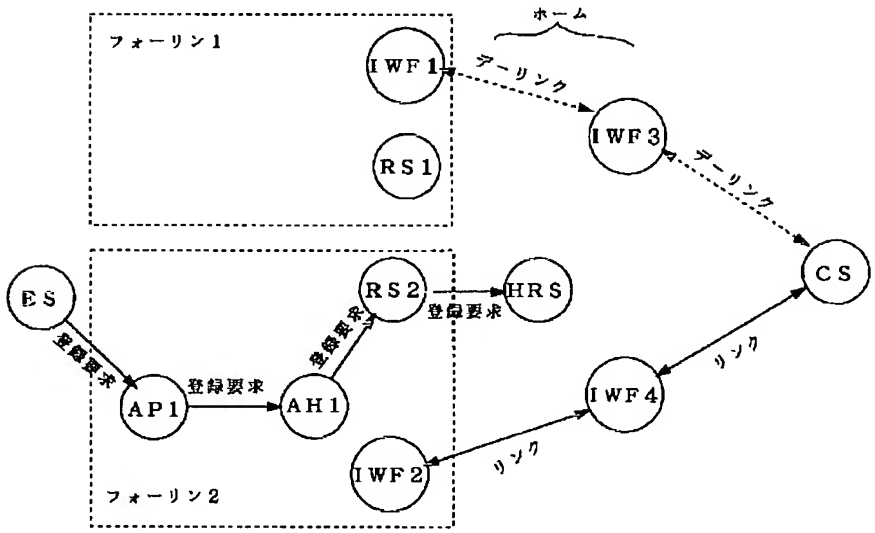
【図３６】


フォーリン
ホーム
IWF２
AP１
登録要求
AH１
登録要求
登録要求
リンク
MS
RS１
HRS
登録要求
IWF３
CS
フォーリン
IWF１

【図３７】



【図３８】



フロントページの続き

(51)Int.Cl.[6]	識別記号	FI	
H04M 11/00	303	H04L 11/20	102D
H04Q 7/34		H04Q 7/04	C

(72)発明者　ギリシュ　ライ
アメリカ合衆国　60103　イリノイズ，バートレット，レディ　スミス　ロード　523

【外国語明細書】

1. Title of Invention

MOBILITY MANAGEMENT SYSTEM

2. Claims

1. A communications system comprising:

a network that includes a first registration server and first and second access points and a first access hub, the network initially communicating data frames between a first mobile end system and the first access hub through the first access point;

wherein the first access hub includes a first module to re-register the first mobile end system with the first access hub without informing the first registration server when a registration request is received from the first mobile end system through the second access point;

wherein the first access hub further includes a second module to link the second access point with the first access hub when the mobile end system re-registers through the second access point; and

wherein the first access hub further includes a third module to de-link the first access point from the first access hub when the second access point is linked with the first access hub.

2. The system of claim 1, wherein:

the network is regarded as a foreign network and the foreign network further includes second and third access hubs and a first inter-working function, the foreign network initially communicating data frames between a second mobile end system and the first inter-working function through the second access hub;

a home network includes a home registration server;

the first registration server includes a first module to re-register the second mobile end system with the first registration server without informing the home registration server when a registration request is received from the second mobile end system through a third access point and through the third access hub;

the first registration server further includes a second module to comand the third access hub to be linked with the first inter-working function when the second mobile end system re-registers through the third access hub; and

the first registration server further includes a third module to command the second access hub to be de-linked from the first inter-working function after the third access hub is linked with the first inter-working function.

3. The system of claim 2, wherein:

the foreign network further includes a fourth access hub and second and third inter-working functions;

the home network further includes a fourth inter-working function, the foreign network initially communicating data frames between a third mobile end system and the fourth inter-working function through the second inter-working function, the home network initially communicating data frames between the fourth inter-working function and a first communications server;

the home registration server includes a first module to re-register the third mobile end system with the home registration server without de-linking the fourth inter-working function from the first communications server when a registration request is received from the third mobile end system through a fourth access point and through the fourth access hub and through the first registration server, the first module recognizing an indication in the registration request of a change from the second inter-working function to the third inter-working function;

the home registration server further includes a second module to comand the fourth inter-working function to be linked with the third inter-working function when the third mobile end system re-registers through the fourth access hub; and

the home registration server further includes a third module to comand the fourth inter-working function to be de-linked from the second inter-working function after the third inter working function is linked with the fourth inter-working function.

4. The system of claim 3, wherein:

the foreign network is regarded as a first foreign network and the first foreign network further includes a fifth inter working function;

a second foreign network includes a second registration server and a fifth access hub and a sixth inter-working function;

the home network further includes a seventh inter-working function, the first foreign network initially communicating data frames between a fourth mobile end system and the seventh inter-working function through the fifth inter-working function, the home network initially communicating data frames between the seventh inter-working function and a second communications server;

the home registration server further includes a fourth module to re-register the fourth mobile end system with the home registration server without de-linking the seventh inter-working function from the second communications server when a registration request is received from the fourth mobile end system through a fifth access point and through the fifth access hub and through the second registration server to the home registration server;

the home registration server further includes a fifth module to command the seventh inter-working function to be linked with the sixth inter-working function when the fourth mobile end system re-registers through the fifth access hub; and

the home registration server further includes a sixth module to command the seventh inter-working function to be de-linked from the fifth inter-working function after the sixth inter-working function is linked with the seventh inter-working function.

5. The system of claim 3, wherein:

the foreign network is regarded as a first foreign network and the first foreign network further includes a fifth inter-working function;

a second foreign network includes a second registration server and a fifth access hub and a sixth inter working function;

the home network further includes seventh and eighth inter-working functions, the first foreign network initially communicating data frames between a fourth mobile end system and seventh inter-working function through the fifth inter-working function, the home network initially communicating data frames between the seventh inter-working function and a second communications server;

the home registration server further includes a fourth module to re register the fourth mobile end system with the home registration server when a registration request is received from the fourth mobile end system through a fifth access point and through the fifth access hub and through the second registration server to the home registration server;

the home registration server further includes a fifth module to command the eighth inter-working function to be linked with the sixth inter-working function when the fourth mobile end system re-registers through the fifth access hub;

the home registration server further includes a sixth module to command the eighth inter-working function to be linked with the second communications server;

the home registration server further includes a seventh module to command the seventh inter-working function to be de-linked from the second communications server; and

the home registration server further includes an eighth module to command the seventh inter-working function to be de-linked from the fifth inter-working function after the eighth inter-working function is linked with the sixth inter-working function.

6. A communications system comprising:

a foreign network that includes a first registration server and first and second access hubs and a first inter-working function, the foreign network initially communicating data frames between a first mobile end system and the first inter-working function through the first access hub;

a home network that includes a home registration server;

wherein the first registration server includes a first module to re-register the first mobile end system with the first registration server without informing the home registration server when a registration request is received from the first mobile end system through a first access point and through the second access hub to the first registration server;

wherein the first registration server further includes a second module to command the second access hub to be linked with the first inter-working function when the first mobile end system re-registers through the second access hub; and

wherein the first registration server further includes a third module to command the first access hub to be de-linked from the first inter-working function after the second access hub is linked with the first inter-working function.

7. The system of claim 6, wherein:

the foreign network further includes a third access hub and second and third inter-working functions;

the home network further includes a fourth inter-working function, the foreign network initially communicating data frames between a second mobile end system and the fourth inter-working function through the second inter-working function, the home network initially communicating data frames between the fourth inter-working function and a first communications server;

the home registration server includes a first module to re-register the second mobile end system with the home registration server without de-linking the fourth inter-working function from the first communications server when a registration request is received from the second mobile end system through a second access point and through the third access hub and through the first registration server to the home registration server, the first module recognizing an indication in the registration request of a change from the second inter-working function to the third inter-working function;

the home registration server further includes a second module to command the third inter-working function to be linked with the fourth inter-working function when the second mobile end system re-registers through the third access hub; and

the home registration server further includes a third module to command the second inter-working function to be de-linked from the fourth inter-working function after the third inter-working function is linked with the fourth inter-working function.

8. The system of claim 7, wherein:

the foreign network is regarded as a first foreign network and the first foreign network further includes a fifth inter-working function;

a second foreign network includes a second registration server and a fourth access hub and a sixth inter-working function;

the home network further includes a seventh inter-working function, the first foreign network initially communicating data frames between a third mobile end system and the seventh inter-working function through the fifth inter-working function, the home network initially communicating data frames between the seventh inter-

working function and a second communications server;

the home registration server further includes a fourth module to re-register the third mobile end system with the home registration server without de-linking the seventh inter-working function from the second communications server when a registration request is received from the third mobile end system through a third access point and through the fourth access hub and through the second registration server to the home registration server;

the home registration server further includes a fifth module to command the sixth inter-working function to be linked with the seventh inter-working function when the third mobile end system re-registers through the fourth access hub; and

the home registration server further includes a sixth module to command the fifth inter-working function to be de-linked from the seventh inter-working function after the sixth inter-working function is linked with the seventh inter-working function.

9. The system of claim 7, wherein:

the foreign network is regarded as a first foreign network and the first foreign network further includes a fifth inter-working function;

a second foreign network includes a second registration server and a fourth access hub and a sixth inter-working function;

the home network further includes seventh and eighth inter-working functions, the first foreign network initially communicating data frames between a third mobile end system and seventh inter-working function through the fifth inter-working function, the home network initially communicating data frames between the seventh inter-working function and a second communications server;

the home registration server further includes a fourth module to re-register the third mobile end system with the home registration server when a registration request is received from the third mobile end system through a third access point and through the fourth access hub and through the second registration server to the home registration server;

the home registration server further includes a fifth module to command the eighth inter-working function to be linked with the sixth inter-working function when the third mobile end system re registers through the fourth access hub;

the home registration server further includes a sixth module to command the eighth inter-working function to be linked with the second communications server;

the home registration server further includes a seventh module to command the seventh inter-working function to be de-linked from the second communications server; and

the home registration server further includes an eighth module to command the seventh inter-working function to be de-linked from the fifth inter-working function after the eighth inter-working function is linked with the sixth inter-working function.

10. A communications system comprising:

a foreign network that includes a first registration server and a first access hub and first and second inter-working functions;

a home network that include a home registration server and a third inter-working function, the foreign network initially communicating data frames between a first mobile end system and the third inter-working function through the first inter-working function, the home network initially communicating data frames between the third inter-working function and the first communications server;

wherein the home registration server includes a first module to re-register the first mobile end system with the home registration server without de-linking the third inter-working function from the first communications server when a registration request is received from the first mobile end system through a first access point and through the first access hub and through the first registration server to the home registration server, the first module recognizing an indication in the registration request of a change from the first inter-working function to the second inter-working function;

wherein the home registration server further includes a second module to command the second inter-working function to be linked with the third inter-working function when the first mobile end system re-registers through the first access hub; and

wherein the home registration server further includes a third module to command the first inter-working function to be de-linked from the third inter working function after the second inter-working function is linked with the third inter-working function.

11. The system of claim 10, wherein:

the foreign network is regarded as a first foreign network and the first foreign network further includes fourth inter-working function;

a second foreign network includes a second registration server and a second access hub and a fifth inter-working function;

the home network further includes a sixth inter-working function, the first foreign network initially communicating data frames between a second mobile end system and the sixth inter-working function through the fourth inter-working function, the home network initially communicating data frames between the sixth inter-working function and a second communications server;

the home registration server further includes a fourth module to re-register the second mobile end system with the home registration server without de-linking the sixth inter-working function from the second communications server when a registration request is received from the second mobile end system through a second access point and through the second access hub and through the second registration server to the home registration server;

the home registration server further includes a fifth module to command the fifth inter-working function to be linked with the sixth inter-working function when the second mobile end system re-registers through the second access hub; and

the home registration server further includes a sixth module to command the fourth inter-working function to be de-linked from the sixth inter-working function after the fifth inter-working function is linked with the sixth inter-working function.

12. The system of claim 10, wherein:

the foreign network is regarded as a first foreign network and the first foreign network further includes a fourth inter-working function;

a second foreign network includes a second registration server and a second access hub and a fifth inter-working function;

the home network further includes sixth and seventh inter-working functions, the first foreign network initially communicating data frames between a second mobile end system and the sixth inter-working function through the fourth inter-working function, the home network initially communicating data frames between the sixth inter-working function and a second communications server;

the home registration server further includes a fourth module to re-register the second mobile end system with the home registration server when a registration request is received from the second mobile end system through a second access point and through the second access hub and through the second registration server to the home registration server;

the home registration server further includes a fifth module to command the fifth inter-working function to be linked with the seventh inter-working function when the second mobile end system re-registers through the second access hub;

the home registration server further includes a sixth module to command the seventh inter-working function to be linked with the second communications server;

the home registration server further includes a seventh module to command the sixth inter-working function to be de-linked from the second communications server; and

the home registration server further includes an eighth module to command the sixth inter-working function to be de-linked from the fourth inter-working function after the seventh inter-working function is linked with the fifth inter-working function.

13. A communications system comprising:

a first foreign network that includes a first registration server and a first inter-working function;

a second foreign network that includes a second registration server and a first access hub and a second inter-working function;

a home network that includes a home registration server and a third inter-working function, the first foreign network initially communicating data frames between a first mobile end system and the third inter-working function through the first inter-working function, the home network initially communicating data frames between the third inter-working function and the first communications server;

wherein the home registratation server includes a first module to re-register the first mobile end system with the home registration server without de-linking the third inter-working function from the first communications server when a registration request is received from the first mobile end system through a first access point and through the first access hub and through the second registration server to the home registration server;

wherein the home registratation server further includes a second module to command the third inter-working function to be linked with the second inter-working function when the first mobile end system re-registers through the first access hub; and

wherein the home registratation server further includes a third module to command the third inter-working function to be de-linked from the first inter-working function after the third inter-working function is linked with the second inter-working function.

14. A communications system comprising:

a first foreign network that includes a first registration server and a first inter-working function;

a second foreign network that includes a second registration server and a first access hub and a second inter-working function;

a home network that includes a home registration server and third and fourth inter-working functions, the first foreign network initially communicating data frames between a first mobile end system and the third inter-working function through the first inter-working function, the home network initially communicating data frames between the third inter-working function and the first communications server;

wherein the home registratation server includes a first module to re-register the first mobile end system with the home registration server when a registration request is received from the first mobile end system through a first access point and through the first access hub and through the second registration server to the home registration server;

wherein the home registratation server further includes a second module to command the fourth inter-working function to be linked with the second inter-working function when the first mobile end system re-registers through the first access hub;

wherein the home registratation server further includes a third module to command the fourth inter-working function to be linked with the first communications server;

wherein the home registratation server further includes a fourth module to command the third inter-working function to be de-linked from the first communications server when the fourth inter-working function is linked with the first communications server; and

wherein the home registratation server further includes a fifth module to command the third inter working function to be de-linked from the first inter-working function after the fourth inter-working function is linked with the second inter-working function.

15. In a network that includes a first registration server and first and second access points and a first access hub, a method of handing off a connection of a first mobile end system with the first access hub, the method comprising steps of:

initially communicating data frames between the first mobile end system and the first access hub through the first access point;

sending a registration request from the first mobile end system through the second access point to the first access hub to re-register the first mobile end system with the first access hub without informing the first registration server when the first mobile end system moves and re-registers through the second access point;

linking the second access point with the first access hub when the first mobile end system re-registers through the second access point; and

de-linking the first access point from the first access hub when the second access point is linked with the first access hub.

16. The method of claim 15, wherein:

the network is regarded as a foreign network and the foreign network further includes second and third access hubs and a first inter-working function;

a home network includes a home registration server;

the method further includes a step of initially communicating data frames between a second mobile end system and the first inter-working function through the second access hub;

the method further includes a step of sending a registration request from the second mobile end system through a third access point and through the third access hub to the first registration server to re-register the second mobile end system with the first registration server without informing the home registration server when the second mobile end system moves and re-registers through the third access hub;

the method further includes a step of linking the third access hub with the first inter-working function when the second mobile end system re-registers through the third access hub; and

the method further includes a step of de-linking the second access hub from the first inter-working function after the third access hub is linked with the first inter-working function.

17. The method of claim 16, wherein:

the foreign network further includes a fourth access hub and second and third inter-working functions;

the home network further includes a fourth inter-working function;

the method further includes a step of initially communicating data frames between a third mobile end system and the fourth inter-working function through the second inter-working function;

the method further includes a step of initially communicating data frames between the fourth inter-working function and a first communications server;

the method further includes a step of sending a registration request from the third mobile end system through a fourth access point and through the fourth access hub and through the first registration server to the home registration server to re register the third mobile end system with the home registration server without de-linking the fourth inter-working function from the first communications server when the third mobile end system moves and re-registers through the fourth access hub, the step of sending the registration request from the first registration server to the home registration server including a sub-step of sending an indication of a change from the second inter-working function to the third inter-working function;

the method further includes a step of linking the third inter-working function with the fourth inter-working function when the third mobile end system re-registers through the fourth access hub; and

the method further includes a step of de-linking the second inter-working function from the fourth inter-working function after the third inter-working function is linked with the fourth inter-working function.

18. The method of claim 17, wherein:

the foreign network is regarded as a first foreign network and the first foreign network further includes a fifth inter-working function;

a second foreign network includes a second registration server and a fifth access hub and a sixth inter-working function;

the home network further includes a seventh inter-working function;

the method further includes a step of initially communicating data frames between a fourth mobile end system and the seventh inter-working function through the fifth inter-working function;

the method further includes a step of initially communicating data frames between the seventh inter-working function and a second communications server;

the method further includes a step of sending a registration request from the fourth mobile end system through a fifth access point and through the fifth access hub and through the second registration server to the home registration server to re-register the fourth mobile end system with the home registration server without de-linking the seventh inter-working function from the second communications server when the fourth mobile end system moves and re-registers through the fifth access hub;

the method further includes a step of linking the sixth inter-working function with the seventh inter-working function when the fourth mobile end system re-registers through the fifth access hub; and

the method further includes a step of de-linking the fifth inter-working function from the seventh inter-working function after the sixth inter-working function is linked with the seventh inter-working function.

19. The method of claim 17, wherein:

the foreign network is regarded as a first foreign network and the first foreign network further includes a fifth inter-working function;

a second foreign network includes a second registration server and a fifth access hub and a sixth inter-working function;

the home network further includes seventh and eighth inter-working functions;

the method further includes a step of initially communicating data frames between a fourth mobile end system and seventh inter-working function through the fifth inter-working function;

the method further includes a step of initially communicating data frames between the seventh inter-working function and a second communications server;

the method further includes a step of sending a registration request from the fourth mobile end system through a fifth access point and through the fifth access hub and through the second registration server to the home registration server to re-register the fourth mobile end system with the home registration server when the fourth mobile end system moves and re-registers through the fifth access hub;

the method further includes a step of linking the eighth inter-working function with the sixth inter-working function when the fourth mobile end system re-registers through the fifth access hub;

the method further includes a step of linking the eighth inter-working function with the second communications server;

the method further includes a step of de-linking the seventh inter-working function from the second communications server; and

the method further includes a step of de-linking the seventh inter-working function from the fifth inter-working function after the eighth inter-working function is linked with the sixth inter-working function.

20. In a home network with a home registration server and a foreign network that includes a first registration server and first and second access hubs and a first inter-working function, a method of handing off a connection of a first mobile end system with the first inter-working function, the method comprising steps of:

initially communicating data frames between the first mobile end system and the first inter-working function through the first access hub;

sending a registration request from the first mobile end system through a first access point and through the second access hub to the first registration server to re-register the first mobile end system with the first registration server without informing the home registration server when the first mobile end system moves and re-registers through the second access hub;

linking the second access hub with the first inter-working function when the first mobile end system re-registers through the second access hub; and

de-linking the first access hub from the first inter-working function after the second access hub is linked with the first inter-working function.

21. The method of claim 20, wherein:

the foreign network further includes a third access hub and second and third inter-working functions;

the home network further includes a fourth inter-working function;

the method further includes a step of initially communicating data frames between a second mobile end system and the fourth inter working function through the second inter-working function;

the method further includes a step of initially communicating data frames between the fourth inter-working function and a first communications server;

the method further includes a step of sending a registration request from the second mobile end system through a second access point and through the third access hub and through the first registration server to the home registration server to re-register the second mobile end system with the home registration server without de-linking the fourth inter-working function from the first communications server when the second mobile end system moves and re-registers through the third access hub, the step of sending the registration request from the first registration server to the home registration server including a sub-step of sending an indication of a change from the second inter-working function to the third inter-working function;

the method further includes a step of linking the third inter-working function with the fourth inter-working function when the second mobile end system re-registers through the third access hub; and

the method further includes a step of de-linking the second inter-working function from the fourth inter-working function after the third inter-working function is linked with the fourth inter-working function.

22. The method of claim 21, wherein:

the foreign network is regarded as a first foreign network and the first foreign network further includes a fifth inter-working function;

a second foreign network includes a second registration server and a fourth access hub and a sixth inter-working function;

the home network further includes a seventh inter-working function;

the method further includes a step of initially communicating data frames between a third mobile end system and the seventh inter-working function through the fifth inter-working function;

the method further includes a step of initially communicating data frames between the seventh inter-working function and a second communications server;

the method further includes a step of sending a registration request from the third mobile end system through a third access point and through the fourth access hub and through the second registration server to the home registration server to re-register the third mobile end system with the home registration server without de-linking the seventh inter-working function from the second communications server when the third mobile end system moves and re-registers through the fourth access hub;

the method further includes a step of linking the sixth inter-working function with the seventh inter-working function when the third mobile end system re-registers through the fourth access hub; and

the method further includes a step of de-linking the fifth inter-working function from the seventh inter-working function after the sixth inter-working function is linked with the seventh inter-working function.

23. The method of claim 21, wherein:

the foreign network is regarded as a first foreign network and the first foreign network further includes a fifth inter-working function;

a second foreign network includes a second registration server and a fourth access hub and a sixth inter-working function;

the home network further includes seventh and eighth inter-working functions;

the method further includes a step of initially communicating data frames between a third mobile end system and seventh inter-working function through the fifth inter-working function;

the method further includes a step of initially communicating data frames between the seventh inter-working function and a second communications server;

the method further includes a step of sending a registration request from the third mobile end system through a third access point and through the fourth access hub and through the second registration server to the home registration server to re-register the third mobile end system with the home registration server when the third mobile end system moves and re-registers through the fourth access hub;

the method further includes a step of linking the eighth inter-working function with the sixth inter-working function when the third mobile end system re-registers through the fourth access hub;

the method further includes a step of linking the eighth inter-working function with the second communications server;

the method further includes a step of de-linking the seventh inter-working function from the second communications server; and

the method further includes a step of de-linking the seventh inter-working function from the fifth inter-working function after the eighth inter-working function is linked with the sixth inter-working function.

24. In a home network with a home registration server and a foreign network that includes a first registration server and a first access hub and first and second inter-working functions, the home network further including a third inter-working function,

a method of handing off a connection of a first mobile end system with a first communications server, the method comprising steps of:

initially communicating data frames between the first mobile end system and the third inter-working function through the first inter-working function;

initially communicating data frames between the third inter-working function and the first communications server;

sending a registration request from the first mobile end system through a first access point and through the first access hub and through the first registration server to the home registration server to re-register the first mobile end system with the home registration server without de-linking the third inter-working function from the first communications server when the first mobile end system moves and re-registers through the first access hub, the step of sending the registration request from the first registration server to the home registration server including a sub-step of sending an indication of a change from the first inter-working function to the second inter-working function;

linking the second inter-working function with the third inter-working function when the first mobile end system re-registers through the first access hub; and

de-linking the first inter-working function from the third inter-working function after the second inter-working function is linked with the third inter-working function.

25. The method of claim 24, wherein:

the foreign network is regarded as a first foreign network and the first foreign network further includes fourth inter-working function;

a second foreign network includes a second registration server and a second access hub and a fifth inter-working function;

the home network further includes a sixth inter-working function;

the method further includes a step of initially communicating data frames between a second mobile end system and the sixth inter-working function through the fourth inter-working function;

the method further includes a step of initially communicating data frames between the sixth inter-working function and a second communications server;

the method further includes a step of sending a registration request from the second mobile end system through a second access point and through the second access hub and through the second registration server to the home registration server to re-register the second mobile end system with the home registration server without de-linking the sixth inter-working function from the second communications server when the second mobile end system moves and re-registers through the second access hub;

the method further includes a step of linking the fifth inter-working function with the sixth inter-working function when the second mobile end system re-registers through the second access hub; and

the method further includes a step of de-linking the fourth inter-working function from the sixth inter-working function after the fifth inter-working function is linked with the sixth inter-working function.

26. The method of claim 24, wherein:

the foreign network is regarded as a first foreign network and the first foreign network further includes a fourth inter-working function;

a second foreign network includes a second registration server and a second access hub and a fifth inter-working function;

the home network further includes sixth and seventh inter-working functions;

the method further includes a step of initially communicating data frames between a second mobile end system and the sixth inter-working function through the fourth inter-working function;

the method further includes a step of initially communicating data frames between the sixth inter-working function and a second communications server;

the method further includes a step of sending a registration request from the second mobile end system through a second access point and through the second access hub and through the second registration server to the home registration server to re-register the second mobile end system with the home registration server when the second mobile end system moves and re registers through the second access hub;

the method further includes a step of linking the fifth inter-working function with the seventh inter-working function when the second mobile end system re-registers through the second access hub;

the method further includes a step of linking the seventh inter-working function with the second communications server;

the method further includes a step of de-linking the sixth inter-working function from the second communications server; and

the method further includes a step of de-linking the sixth inter-working function from the fourth inter-working function after the seventh inter-working function is linked with the fifth inter-working function.

27. In a home network and first and second foreign networks, the first foreign network including a first registration server and a first inter working function, the second foreign network including a second registration server and a first access hub and a second inter-working function, the home network including a home registration server and a third inter-working function, a method of handing off a connection of a first mobile end system with a first communications server, the method comprising steps of:

initially communicating data frames between a first mobile end system and the third inter-working function through the first inter-working function;

initially communicating data frames between the third inter-working function and the first communications server;

sending a registration request from the first mobile end system through a first access point and through the first access hub and through the second registration server to the home registration server to re-register the first mobile end system with the home registration server without de-linking the third inter-working function from the first communications server when the first mobile end system moves and re-registers through the first access hub;

linking the third inter-working function with the second inter-working function when the first mobile end system re-registers through the first access hub; and

de-linking the third inter-working function from the first inter-working function after the third inter-working function is linked with the second inter-working function.

28. In a home network and first and second foreign networks, the first foreign network including a first registration server and a first inter-working function, the second foreign network including a second registration server and a first access hub and a second inter-working function, the home network including a home registration server and third and fourth inter-working functions, a method of handing off a connection of a first mobile end system with a first communications server, the method comprising steps of:

initially communicating data frames between a first mobile end system and the third inter-working function through the first inter-working function;

initially communicating data frames between the third inter working function and the first communications server;

sending a registration request from the first mobile end system through a first access point and through the first access hub and through the second registration server to the home registration server to re-register the first mobile end system with the home registration server when the first mobile end system moves and re-registers through the first access hub;

linking the fourth inter-working function with the second inter-working function when the first mobile end system re-registers through the first access hub;

linking the fourth inter-working function with the first communications server;

de-linking the third inter-working function from the first communications server when the fourth inter-working function is linked with the first communications server; and

de-linking the third inter-working function from the first inter-working function after the fourth inter-working function is linked with the second inter-working function.

3. Detailed Explanation of the Invention

Background of the Invention

Priority benefit of the October 14, 1997 filing date of provisional application serial number 60/061,915 is hereby claimed.

Field of the Invention

The present invention relates to the management of mobile end systems in a packet switched data network that provides computer users with remote access to the internet and to private intranets using virtual private network services over a high speed, packet switched, wireless data link. In particular, the invention relates to the management of connection handovers when a mobile end system moves from one cell to another.

Description Of Related Art

FIG. 1 depicts three business entities, whose equipment, working together typically provide remote internet access to user computers 2 through user modems 4. User computers 2 and modems 4 constitute end systems.

The first business entity is the telephone company (telco) that owns and operates the dial-up plain old telephone system (POTS) or integrated services data network (ISDN) network. The telco provides the media in the form of public switched telephone network (PSTN) 6 over which bits (or packets) can flow between users and the other two business entities.

The second business entity is the internet service provider (ISP). The ISP deploys and manages one or more points of presence (POPs) 8 in its service area to which end users connect for network service. An ISP typically establishes a POP in

each major local calling area in which the ISP expects to subscribe customers. The POP converts message traffic from the PSTN run by the telco into a digital form to be carried over intranet backbone 10 owned by the ISP or leased from an intranet backbone provider like MCI, Inc. An ISP typically leases fractional or full T1 lines or fractional or full T3 lines from the telco for connectivity to the PSTN. The POPs and the ISP's medium data center 14 are connected together over the intranet backbone through router 12A. The data center houses the ISP's web servers, mail servers, accounting and registration servers, enabling the ISP to provide web content, e-mail and web hosting services to end users. Future value added services may be added by deploying additional types of servers in the data center. The ISP also maintains router 12A to connect to public internet backbone 20. In the current model for remote access, end users have service relationships with their telco and their ISP and usually get separate bills from both. End users access the ISP, and through the ISP, public internet 20, by dialing the nearest POP and running a communication protocol known as the Internet Engineering Task Force (IETF) point-to-point protocol (PPP).

The third business entity is the private corporation which owns and operates its own private intranet 18 through router 12B for business reasons. Corporate employees may access corporate network 18 (e.g., from home or while on the road) by making POTS/ISDN calls to corporate remote access server 16 and running the IETF PPP protocol. For corporate access, end users only pay for the cost of connecting to corporate remote access server 16. The ISP is not involved. The private corporation maintains router 12B to connect an end user to either corporate intranet 18 or public internet 20 or both.

End users pay the telco for the cost of making phone calls and for the cost of a phone line into their home. End users also pay the ISP for accessing the ISP's network and services. The present invention will benefit wireless service providers like Sprint PCS, PrimeCo, etc. and benefit internet service providers like AOL, AT&T Worldnet, etc.

Today, internet service providers offer internet access services, web content services, e-mail services, content hosting services and roaming to end users. Because of low margins and no scope of doing market segmentation based on features and price, ISPs are looking for value added services to improve margins. In the short term, equipment vendors will be able to offer solutions to ISPs to enable them to offer faster access, virtual private networking (which is the ability to use public networks securely as private networks and to connect to intranets), roaming consortiums, push technologies and quality of service. In the longer term, voice over internet and mobility will also be offered. ISPs will use these value added services to escape from the low margin straitjacket. Many of these value added services fall in the category of network services and can be offered only through the network infrastructure equipment. Others fall in the category of application services which require support from the network infrastructure, while others do not require any support from the network infrastructure. Services like faster access, virtual private networking, roaming, mobility, voice, quality of service, quality of service based accounting all need enhanced network infrastructure. The invention described here will be either directly provide these enhanced services or provide hooks so that these services can be added later as future enhancements. Wireless service providers will be able to capture a larger share of the revenue stream. The ISP will be able to offer more services and with better market segmentation.

Summary Of The Invention

The present invention provide end users with remote wireless access to the public internet, private intranets and internet service providers. Wireless access is provided through base stations in a home network and base stations in foreign networks with interchange agreements.

It is an object of the present invention to provide a wireless packet switched data network for end users that divides mobility management into local, micro, macro and global connection handover categories and minimizes handoff updates according to the handover category. It is another object to integrate MAC handoff messages with network handoff messages. It is a further object of the present invention to separately direct registration functions to a registration server and direct routing functions to inter-working function units. It is yet another object to provide an intermediate XTunnel channel between a wireless hub (also called access hub AH) and an inter-working function unit (IWF unit) in a foreign network. It is yet another object to provide an IXTunnel channel between an inter-working function unit in a foreign network and an inter-working function unit in a home network. It is yet another object to enhance the layer two tunneling protocol (L2TP) to support a mobile end system. It is yet another object to perform network layer registration before the start of a PPP communication session.

Detailed Description Of Preferred Embodiments

The present invention provides computer users with remote access to the internet and to private intranets using virtual private network services over a high speed, packet switched, wireless data link. These users are able to access the public internet, private intranets and their internet service providers over a wireless link. The network supports roaming, that is, the ability to access the internet and private intranets using virtual private network services from anywhere that the services offered by the present invention are available. The network targets users running horizontal internet and intranet applications. These applications include electronic mail, file transfer, browser based WWW access and other business applications built around the internet. Because the network will be based on the IETF standards, it is possible to run streaming media protocols like RTP and conferencing protocols like H.323 over it.

Other internet remote access technologies that are already deployed or are in various stages of deployment include: wire line dial-up access based on POTS and ISDN, XDSL access, wireless circuit switched access based on GSM/CDMA/TDMA, wireless packet switched access based on GSM/CDMA/TDMA, cable modems, and satellite based systems. However, the present invention offers a low cost of deployment, ease of maintenance, a broad feature set, scaleability, an ability to degrade gracefully under heavy load conditions and support for enhanced network services like virtual private networking, roaming, mobility and quality of service to the relative benefit of users and service providers.

For wireless service providers who own personal communications system (PCS) spectrum, the present invention will enable them to offer wireless packet switched data access services that can compete with services provided by the traditional wire line telcos who own and operate the PSTN. Wireless service providers may also decide to become internet service providers themselves, in which case, they will own and operate the whole network and provide end to end services to users.

For internet service providers the present invention will allow them to by-pass the telcos (provided they purchase or lease the spectrum) and offer direct end to end services to users, perhaps saving access charges to the telcos, which may increase in the future as the internet grows to become even bigger than it is now.

The present invention is flexible so that it can benefit wireless service providers who are not internet service providers and who just provide ISP, internet or private intranet access to end users. The invention can also benefit service providers who provide wireless access and internet services to end users. The invention can also benefit service providers who provide wireless access and internet services but also allow the wireless portion of the network to be used for access to other ISPs or to private intranets.

In FIG. 2, end systems 32 (e.g., based on, for example, Win 95 personal computer) connect to wireless network 30 using external or internal modems. These modems allow end systems to send and receive medium access control (MAC) frames over air link 34. External modems attach to the PC via a wired or wireless link. External modems are fixed, and, for example, co-located with roof top mounted directional antennae. External modems may be connected to the user's PC using any one of following means: 802.3, universal serial bus, parallel port, infra-red, or even an ISM radio link. Internal modems are preferably PCMCIA cards for laptops and

are plugged into the laptop's backplane. Using a small omni-directional antenna, they send and receive MAC frames over the air link.

Wide-area wireless coverage is provided by base stations 36. The range of coverage provided by base stations 36 depends on factors like link budget, capacity and coverage. Base stations are typically installed in cell sites by PCS (personal communication services) wireless service providers. Base stations multiplex end system traffic from their coverage area to the system's mobile switching center (MSC) 40 over wire line or microwave backhaul network 38.

The invention is independent of the MAC and PHY (physical) layer of the air link and the type of modem. The architecture is also independent of the physical layer and topology of backhaul network 38. The only requirements for the backhaul network are that it must be capable of routing internet protocol (IP) packets between base stations and the MSC with adequate performance. At Mobile Switching Center 40 (MSC 40), packet data inter-working function (IWF) 52 terminates the wireless protocols for this network. IP router 42 connects MSC 40 to public internet 44, private intranets 46 or to internet service providers 46. Accounting and directory servers 48 in MSC 40 store accounting data and directory information. Element management server 50 manages the equipment which includes the base stations, the IWFs and accounting/directory servers.

The accounting server will collect accounting data on behalf of users and send the data to the service provider's billing system. The interface supported by the accounting server will send accounting information in American Management Association (AMA) billing record format over a TCP/IP (transport control protocol/internet protocol) transport to the billing system (which is not shown in the figure).

The network infrastructure provides PPP (point-to-point protocol) service to end systems. The network provides (1) fixed wireless access with roaming (log-in anywhere that the wireless coverage is available) to end systems and (2) low speed mobility and hand-offs. When an end system logs on to a network, in it may request either fixed service (i.e., stationary and not requiring handoff services) or mobile service (i.e., needing handoff services). An end system that does not specify fixed or mobile is regarded as specifying mobile. The actual registration of the end system is the result of a negotiation with a home registration server based on requested level of service, the level of services subscribed to by the user of the end system and the facilites available in the network.

If the end system negotiates a fixed service registration (i.e., not requiring handoff services) and the end system is located in the home network, an IWF (inter working function) is implemented in the base station to relay traffic between the end user and a communications server such as a PPP server (i.e., the point with which to be connected, for example, an ISP PPP server or a corporate intranet PPP server or a PPP server operated by the wireless service provider to provide customers with direct access to the public internet). It is anticipated that perhaps 80% of the message traffic will be of this category, and thus, this architecture distributes IWF processing into the base stations and avoids message traffic congestion in a central mobile switching center.

If the end system requests mobile service (from a home network or a foreign network) or if the end system request roaming service (i.e., service from the home network through a foreign network), two IWFs are established: a serving IWF typically established in the base station of the network to which the end system is attached (be it the home network or a foreign network) and a home IWF typically

established in mobile switching center MSC of the home network. Since this situation is anticipated to involve only about 20% of the message traffic, the message traffic congestion around the mobile switching center is minimized. The serving IWF and the wireless hub may be co-located in the same nest of computers or may even be programmed in the same computer so that a tunnel using an XTunnel protocol need not be established between the wireless hub and the serving IWF.

However, based on available facilities and the type and quality of service requested, a serving IWF in a foreign network may alternatively be chosen from facilities in the foreign MSC. Generally, the home IWF becomes an anchor point that is not changed during the communications session, while the serving IWF may change if the end system moves sufficiently.

The base station includes an access hub and at least one access point (be it remote or collocated with the access hub). Typically, the access hub serves multiple access points. While the end system may be attached to an access point by a wire or cable according to the teachings of this invention, in a preferred embodiment the end system is attached to the access point by a wireless "air link", in which case the access hub is conveniently referred to as a wireless hub. While the access hub is referred to as a "wireless hub" throughout the description herein, it will be appreciated that an end system coupled through an access point to an access hub by wire or cable is an equivalent implementation and his contemplated by the term "access hub".

In the invention, an end system includes an end user registration agent (e.g., software running on a computer of the end system, its modem or both) that communicates with an access point, and through the access point to a wireless hub. The wireless hub includes a proxy registration agent (e.g., software running on a

processor in the wireless hub) acting as a proxy for the end user registration agent. Similar concepts used in, for example, the IETF proposed Mobile IP standard are commonly referred to as a foreign agent (FA). For this reason, the proxy registration agent of the present invention will be referred to as a foreign agent, and aspects of the foreign agent of the present invention that differ from the foreign agent of Mobile IP are as described throughout this description.

Using the proxy registration agent (i.e., foreign agent FA) in a base station, the user registration agent of an end system is able to discover a point of attachment to the network and register with a registration server in the MSC (mobile switching center) of the home network. The home registration server determines the availability of each of the plural inter-working function modules (IWFs) in the network (actually software modules that run on processors in both the MSC and the wireless hubs) and assigns IWF(s) to the registered end system. For each registered end system, a tunnel (using the *XTunnel* protocol) is created between the wireless hub in the base station and an inter-working function (IWF) in the mobile switching center (MSC), this tunnel transporting PPP frames between the end system and the IWF.

As used herein, the XTunnel protocol is a protocol that provides in-sequence transport of PPP data frames with flow control. This protocol may run over standard IP networks or over point-to-point networks or over switched networks like ATM data networks or frame relay data networks. Such networks may be based on T1 or T3 links or based on radio links, whether land based or space based. The XTunnel protocol may be built by adapting algorithms from L2TP (level 2 transport protocol). In networks based on links where lost data packets may be encountered, a re-transmission feature may be a desirable option.

The end system's PPP peer (i.e., a communications server) may reside in the IWF or in a corporate intranet or ISP's network. When the PPP peer resides in the IWF, an end system is provided with direct internet access. When the PPP peer resides in an intranet or ISP, an end system is provided with intranet access or access to an ISP. In order to support intranet or ISP access, the IWF uses the layer two tunneling protocol (L2TP) to connect to the intranet or ISP's PPP server. From the point of view of the intranet or ISP's PPP server, the IWF looks like a network access server (NAS). PPP traffic between the end system and the IWF is relayed by the foreign agent in the base station.

In the reverse (up link) direction, PPP frames traveling from the end system to the IWF are sent over the MAC and air link to the base station. The base station relays these frames to the IWF in the MSC using the *XTunnel* protocol. The IWF delivers them to a PPP server for processing. For internet access, the PPP server may be in the same machine as the IWF. For ISP or intranet access, the PPP server is in a private network and the IWF uses the layer two tunneling protocol (L2TP) to connect to it.

In the forward (down link) direction, PPP frames from the PPP server are relayed by the IWF to the base station using the *XTunnel* protocol. The base station de-tunnels down link frames and relays them over the air link to the end system, where they are processed by the end system's PPP layer.

To support mobility, support for hand-offs are included. The MAC layer assists the mobility management software in the base station and the end system to perform hand-offs efficiently. Hand-offs are handled transparently from the peer PPP entities and the L2TP tunnel. If an end system moves from one base station to

another, a new *XTunnel* is created between the new base station and the original IWF. The old *XTunnel* from the old base station will be deleted. PPP frames will transparently traverse the new path.

The network supports roaming (i.e., when the end user connects to its home wireless service provider through a foreign wireless service provider). Using this feature, end systems are able to roam away from the home network to a foreign network and still get service, provided of course that the foreign wireless service provider and the end system's home wireless service provider have a service agreement.

In FIG. 3, roaming end system 60 has traveled to a location at which foreign wireless service provider 62 provides coverage. However, roaming end system 60 has a subscriber relationship with home wireless service provider 70. In the present invention, home wireless service provider 70 has a contractual relationship with foreign wireless service provider 62 to provide access services. Therefore, roaming end system 60 connects to base station 64 of foreign wireless service provider 62 over the air link. Then, data is relayed from roaming end system 60 through base station 64, through serving IWF 66 of foreign wireless service provider 62, to home IWF 72 of home wireless service provider 70, or possibly through home IWF 72 of home wireless service provider 70 to internet service provider 74.

An inter-service provider interface, called the I-interface, is used for communications across wireless service provider (WSP) boundaries to support roaming. This interface is used for authenticating, registering and for transporting the end system's PPP frames between the foreign WSP and the home WSP.

PPP frames in the up link and the down link directions travel through the end system's home wireless service provider (WSP). Alternatively, PPP frames directly transit from the foreign WSP to the destination network. The base station in the

foreign WSP is the end system's point of attachment in the foreign network. This base station sends (and receives) PPP frames to (and from) a serving IWF in the foreign WSP's mobile switching center. The serving IWF connects over the I-interface to the home IWF using a layer two tunnel to transport the end system's PPP frames in both directions. The serving IWF in the foreign WSP collects accounting data for auditing. The home IWF in the home WSP collects accounting data for billing.

During the registration phase, a registration server in the foreign WSP determines the identity of the roaming end system's home network. Using this information, the foreign registration server communicates with the home registration server to authenticate and register the end system. These registration messages flow over the I-interface. Once the end system has been authenticated and registered, a layer two tunnel is created between the base station and the serving IWF using the *XTUNNEL* protocol and another layer two tunnel is created between the serving IWF and the home IWF over the I-interface. The home IWF connects to the end system's PPP peer as before, using L2TP (level 2 tunnel protocol). During hand-offs, the location of the home IWF and the L2TP tunnel remains fixed. As the end system moves from one base station to another base station, a new tunnel is created between the new base station and the serving IWF and the old tunnel between the old base station and the serving IWF is deleted. If the end system moves far enough, so that a new serving IWF is needed, a new tunnel will be created between the new serving IWF and the home IWF. The old tunnel between the old serving and the home will be deleted.

To support roaming, the I-interface supports authentication, registration and data transport services across wireless service provider boundaries. Authentication and registration services are supported using the IETF Radius protocol. Data transport services to transfer PPP frames over a layer two tunnel are supported using the *I-XTunnel* protocol. This protocol is based on the IETF L2TP protocol.

As used in this description, the term home IWF refers to the IWF in the end system =s home network. The term serving IWF refers to the IWF in the foreign network which is temporarily providing service to the end system. Similarly, the term home registration server refers to the registration server in the end system's home network and the term foreign registration server refers to the registration server in the foreign network through which the end system registers while it is roaming.

The network supports both fixed and dynamic IP address assignment for end systems. There are three types of IP addresses that need to be considered. Two are associated with mobile IP and the third is associated with PPP. The mobile IP RFC mandates that an end system using mobile IP have a fixed home address. Mobile IP also mandates that a care-of-address be used as the end point of the mobile IP tunnel (*XTunnel* in our case). For the present network, the care-of-address used for mobile IP tunneling (i.e. the *XTunnel*) is the IP address of the base station. The use of the fixed home address is deprecated for the network. In mobile IP registration request packets, the value of the home address field is set to 0.0.0.0. A structured User-Name field in the simplified mail transfer protocol (SMTP) format is added to the mobile IP registration request packet. This is of the form *user@domain*. The domain sub-field is used to identify the user's home domain and is a fully qualified domain name. The user sub-field is used to identify the user in the home domain. The User-

Name is stored on the end system and in the subscriber data-base at the MSC and is assigned to the user when he or she subscribes to the service. The domain sub-field of the User-Name is used during roaming to identify roaming relationships and the home registration server for purposes of registration and authentication.

The PPP IPCP is used to negotiate the IP address for the end system. Using IP configuration protocol IPCP, the end system is able to negotiate a fixed or dynamic IP address.

Although the use of the structured user-name field and the non-use of the home address is a feature that characterizes the present invention over a known mobile IP, the network may be enhanced to also support end systems that have no user-name and only a non-null home address, if mobile IP and its use in conjunction with PPP end systems becomes popular. The PPP server may be configured by the service provider to assign IP addresses during the IPCP address assignment phase that are the same as the end system's home address. In this case, the home address and the IPCP assigned IP address will be identical.

In FIG. 4, base station 64 and air links from end systems form wireless sub-network 80 that includes the air links for end user access, at least one base station (e.g., station 64) and at least one backhaul network (e.g., 38 of FIG. 2) from the base station to MSC 40 (FIG.2). The wireless sub-network architecture of, for example, a 3-sectored base station includes the following logical functions.

1. *Access point function.* Access points 82 perform MAC layer bridging and MAC layer association and dissociation procedures. An access point includes a processor (preferably in the form of custom

application specific integrated circuit ASIC), a link to a wireless hub (preferably in the form of an Ethernet link on a card or built into the ASIC), a link to an antenna (preferably in the form of a card with a data modulator/demodulator and a transmitter/receiver), and the antenna to which the end system is coupled. The processor runs software to perform a data bridging function and various other functions in support of registration and mobility handovers as further described herein. See discussion with respect to FIGS. 7, 8 and 11.

Access points (APs) take MAC layer frames from the air link and relay them to a wireless hub and vice versa. The MAC layer association and disassociation procedures are used by APs to maintain a list of end system MAC addresses in their MAC address filter table. An AP will only perform MAC layer bridging on behalf of end systems whose MAC addresses are present in the table. An access point and its associated wireless hub are typically co-located. In its simpliest form, an access point is just a port into a wireless hub. When the APs and the wireless hub are co-located in the same cell site, they may be connected together via a IEEE 802.3 link. Sometimes, access points are located remotely from the wireless hub and connected via a long distance link like a wired T1 trunk or even a wireless trunk. For multi-sector cells, multiple access points (i.e., one per sector) are used.

2. *Wireless hub function.* Wireless hub 84 performs the foreign agent (FA) procedures, backhaul load balancing (e.g., over multiple T1's), backhaul network interfacing, and the *xtunnel* procedures. When

support for quality of service (QOS) is present, the wireless hub implements the support for QOS by running the *xtunnel* protocol over backhauls with different QOS attributes. In a multi-sector cell site, a single wireless hub function is typically shared by multiple access points.

A wireless hub includes a processor, a link to one or more access points (preferably in the form of an Ethernet link on a card or built into an ASIC), and a link to a backhaul line. The backhaul line is typically a T1 or T3 communications line that terminates in the mobile switching center of the wireless service provider. The link to the backhaul line formats data into a preferred format, for example, an Ethernet format, a frame relay format or an ATM format. The wireless hub processor runs software to support data bridging and various other functions as described herein. See discussion with respect to FIGS. 9, 10 and 11.

The base station design supports the following types of cell architectures.

1. *Local AP architecture.* In a local AP architecture, access points have a large (> = 2km, typically) range. They are co-located in the cell site with the wireless hub (FIG. 4). Access points may be connected to the wireless hub using an IEEE 802.3 network or may be directly plugged into the wireless hub's backplane or connected to the wireless hub using some other mechanism (e.g. universal serial bus, printer port, infra-red, etc.). It will be assumed that the first alternative is used for the rest of this discussion. The cell site may be omni or

sectored by adding multiple access points and sectored antennas to a wireless hub.

2. *Remote AP architecture.* In a remote AP architecture, access points usually have a very small range, typically around 1 km radius. They are located remotely (either indoors or outdoors) from the wireless hub. A T1 or a wireless trunk preferably links remote access points to the cell site where the wireless hub is located. From the cell site, a wire line backhaul or a microwave link is typically used to connect to the IWF in the MSC. If wireless trunking between the remote AP and the wireless hub is used, omni or sectored wireless radios for trunking are utilized. The devices for trunking to remote access points are preferably co-located with the wireless hub and may be connected to it using an IEEE 802.3 network or may be directly plugged into the wireless hub=s backplane. These devices will be referred to by the term *trunk AP*.

3. *Mixed AP architecture.* In a mixed architecture, the wireless sub-network will have to support remote and local access points. Remote access points may be added for hole filling and other capacity reasons. As described earlier, T1 or wireless trunks may be used to connect the remote AP to the wireless hub.

FIG. 5 shows a cell with three sectors using local APs only. The access points and the wireless hub are co-located in the base station and are connected to each other with 802.3 links.

FIG. 6 shows an architecture with remote access points 82 connected to

wireless hub 84 using wireless trunks 86. Each trunk access point in the base station provides a point to multi-point wireless radio link to the remote micro access points (R-AP in figure). The remote access points provide air link service to end systems. The wireless hub and the trunk access points are co-located in the base station and connected together via 802.3 links. This figure also shows remote access points 82R connected to the wireless hub via point to point T1 links. In this scenario, no trunk APs are required.

To support all of the above cell architectures and the different types of access points that each cell might use, the network architecture follows the following rules:

1. Access points function as MAC layer bridges. Remote access points perform MAC bridging between the air link to the end systems and the wireless or T1 trunk to the cell site. Local access points perform MAC bridging between the air link to the end systems and the wireless hub.

2. Trunk access points also function as MAC layer bridges. They perform MAC bridging between the trunk (which goes to the access points) and the wireless hub.

3. The wireless hub is connected to all co-located MAC bridges (i.e. local access points or trunk access points) using a 802.3 link initially.

Additionally, where local access points or remote access points with T1 trunks are used, the following rules are followed.

1. Local access points are co-located with the wireless hub and connected to it using point to point 802.3 links or a shared 802.3 network. The first approach is used if the access points can not perform intelligent MAC layer bridging functions or if intelligent MAC layer bridging is deemed too inefficient. Remote access points are connected to the wireless hub using point to point T1 trunks.

2. Sectorization is supported by adding access points with sectored antennas to the cell site.

3. End system registration is done using mobile IP techniques. For each access point connected to the wireless hub, there is a foreign agent executing in the wireless hub. MAC layer association procedures are used to keep the MAC address filter tables of the access points up to date and to perform MAC layer bridging efficiently. The wireless hub participates in MAC association functions so that only valid MAC addresses are added to the MAC address filter tables of the access points.

4. The foreign agent in the wireless hub relays frames from the access points to the MSC IWF and vice versa using the *xtunnel* protocol. The MAC address filter table is used to filter out those unicast MAC data frames whose MAC addresses are not present in the table. The APs always forward MAC broadcast frames and MAC frames associated with end system registration functions regardless of the contents of the MAC address filter table.

5. Local access points use ARP to resolve MAC addresses for routing IP traffic to the wireless hub. Conversely, the wireless hub also uses ARP to route IP packets to access points. UDP/IP is used for network management of access points.

6. Remote access points connected via T1 do not use ARP since the link will be a point to point link.

7. Support for hand-offs uses mobile IP procedures with assistance from the MAC layer.

In a cell architecture using wireless trunks and trunk APs, the following rules are followed.

1. Trunk access points are co-located with the wireless hub and connected to it using point to point 802.3 links. This is done to make it easier to route MAC frames. Note that a shared 802.3 network could also be used, provided the trunk access points can intelligently perform their MAC bridging functions.

2. Wireless trunk sectorization is supported by adding trunk access points with sectored antennas to the cell site.

3. Hand-offs across backhaul sectors are done using mobile IP techniques. For each backhaul sector, there is a foreign agent executing in the wireless hub.

4. The trunk APs do not need to participate in MAC layer end system association and hand off procedures. Their MAC address filter tables will be dynamically programmed by the wireless hub as end systems register with the network. The MAC address filter table is used to filter out unicast MAC frames. Broadcast MAC frames or MAC frames containing registration packets are allowed to always pass through.

5. Trunk APs use ARP to resolve MAC addresses for routing IP traffic to the wireless hub. Conversely, the wireless hub use ARP to route IP packets to trunk APs. UDP/IP is used for network management of trunk APs.

6. In a single wireless trunk sector, MAC association and hand-offs from one access point to another is done using the MAC layer. Using these MAC layer procedures, end systems associate with access points. As end systems move from one access point to another access point, the access points will use a MAC hand off protocol to update their MAC address filter tables. The wireless hub at the cell site provides assistance to access points to perform this function. This assistance includes relaying MAC layer hand off messages (since access points will not be able to communicate directly over the MAC layer with each other) and authenticating the end system for MAC layer registration and hand off and for updating the MAC address filter tables of the access points.

7. The foreign agent for a wireless trunk sector is responsible for relaying frames from its trunk AP to the MSC and vice versa using the *xtunnel* protocol. Thus, the foreign agent for a trunk AP does not care about the location of the end system with respect to access points within that wireless trunk sector. In the down link direction, it just forwards frames from the mobile IP tunnel to the appropriate trunk AP which uses MAC layer bridging to send the frames to all the remote access points attached in that backhaul sector. The access points consult their MAC address filter tables and either forward the MAC frames over the access network or drop the MAC frames. As described above, the MAC address filter tables are kept up to date using MAC layer association and hand off procedures. In the up link direction, MAC frames are forwarded by the access points to the backhaul bridge which forwards them to the foreign agent in the wireless hub using the 802.3 link.

8. ARP is not be used for sending or receiving IP packets to the remote access points. The access points determines the MAC address of the wireless hub using BOOTP procedures. Conversely, the wireless hub is configured with the MAC address of remote access points. UDP/IP is used for network management of access points and for end system association and hand off messages.

IEEE 802.3 links in the cell site may be replaced by higher speed links.

FIG. 7 shows the protocol stack for a local access point. At the base of the stack is physical layer PHY. Physical layer PHY carries data to and from an end system as it is transmitted and received in a stream to and from the data modulator

and demodulator, respectively. When received from an end system, the AP receives data from the physical layer and unpacks it into MAC frames (the MAC layer). The MAC frames are then repacked into an Ethernet physical layer fomat (IEEE 802.3 format) where it is send via the Ethernet link to the wireless hub. When the AP's processor receives data from the wireless hub via its Ethernet link (i.e., the physical layer), the data to be transmitted to an end system, the AP packs the data in a medium access control (MAC) format, and sends the MAC layer data to its modulator to be transmitted to the end system.

In FIG. 8, the MAC and PHY layers to/from the end system of FIG. 7 are replaced by a MAC and PHY for the trunk to the cell site for a remote access point. Specifically, for a T1 trunk, the high level data link control protocol (HDLC protocol) is preferably used over the T1.

FIG. 9 depicts the protocol stack for the wireless hub that bridges the backhaul line and the trunk to the remote access point. The trunk to the remote APs are only required to support remote access points (as distinct from Ethernet coupled access points). The MAC and PHY layers for the wireless trunk to the remote APs provide a point to multipoint link so that one trunk may be used to communicate with many remote APs in the same sector.

The wireless hub bridges the trunk to the remote APs and the backhaul line (e.g., T1 or T3) to the network's mobile switching center (MSC). The protocol stack in the wireless hub implements MAC and PHY layers to the MSC on top of which is implemented an IP layer (Internet Protocol) on top of which is implemented a UDP layer (Universal Datagram Protocal, in combination refered to as UDP/IP) for network management on top of which is implemented an XTunnel protocol. The XTunnel protocol is a new format that includes aspects of

the proposed IETF Mobile IP standard and aspects of the Level 2 Tunnel Protocol (L2TP). The XTunnel protocol is used to communicate from the wireless hub to the MSC and between inter-working functions (IWFs) in different networks or the same network.

In FIG. 10, the protocol stack for the relay function in the base station for supporting remote access points is shown. The relay function includes an interface to the backhaul line (depicted as the wireless hub) and an interface to the remote AP (depicted as a trunk AP). From the point of view of the wireless hub, the trunk AP (depicted in FIGS. 7 and 10) actually behaves like the AP depicted in FIG. 7. Preferably, the base station protocol stacks are split up into a wireless hub and a trunk AP with an Ethernet in between. In an N-sector wireless trunk, there are N wireless trunk APs in the cell site and one wireless hub.

In FIG. 11, the base station protocol stack for a cell architecture using a local AP is shown. The relay function includes an interface to the backhaul line (depicted as the wireless hub) and an air link interface to the end system (depicted as an AP). From the point of view of the wireless hub, the AP (depicted in FIGS. 8 and 11) actually behaves like the trunk AP depicted in FIG. 8. Preferably, the base station protocol stacks are split up into a wireless hub and a trunk AP with an Ethernet in between. In a N-sector cell, there are N access points and a single wireless hub.

The backhaul network from the base station to the MSC has the following attributes.

1. The network is capable of routing IP datagrams between the base station and the MSC.

2. The network is secure. It is not a public internet. Traffic from trusted nodes only are allowed onto the network since the network will be used for not only transporting end system traffic, but also for transporting authentication, accounting, registration and management traffic.

3. The network has the necessary performance characteristics.

In typical application, the service provider is responsible for installing and maintaining the backhaul network on which the equipment is installed.

The base stations supports the following backhaul interfaces for communicating with the MSC.

1. Base stations support IP over PPP with HDLC links using point to point T1 or fractional T3 links.

2. Base stations support IP over frame relay using T1 or fractional T3 links.

3. Base stations support IP over AAL5/ATM using T1 or fractional T3 links.

Since all of the above interfaces are based on IETF standard encapsulations, commercial routers may be used in the MSC to terminate the physical links of the backhaul network. Higher layers are passed on and processed by the various servers and other processors.

End system registration procedures above the MAC layer are supported. In the following, end system registration procedures at the MAC layer are ignored except where they impact the layers above.

End systems may register for service on their home network or from a foreign network. In both scenarios, the end system uses a foreign agent (FA) in the base station to discover a point of attachment to the network and to register. In the former case, the FA is in the end system's home network. In the latter case, the FA is in a foreign network. In either case, the network uses an IWF in the end system's home network as an anchor point (i.e., unchanging throughout the session in spite of mobility). PPP frames to and from the end system travel via the FA in the base station to the IWF in the home network. If the end system is at home, the home IWF is directly connected by means of the *xtunnel* protocol to the base station. If the end system is roaming, a serving IWF in the foreign network is connected to the home IWF over an I-interface. The serving IWF relays frames between the base station and the home IWF. From the home IWF, data is sent to a PPP server which may reside in the same IWF or to a separate server using the L2TP protocol. The separate server may be owned and operated by a private network operator (e.g. ISP or corporate intranet) who is different from the wireless service provider. For the duration of the session, the location of the home IWF and the PPP server remains fixed. If the end system moves while connected, it will have to re-register with a new foreign agent. However, the same home IWF and PPP server continues to be used. A new *xtunnel* is created

between the new FA and the IWF and the old *xtunnel* between the old foreign agent and the IWF is destroyed.

FIG. 12 shows this network configuration for two end systems A and B, both of whose home wireless network is wireless service provider A (WSP-A). One end system is registered from the home wireless network and the other from a foreign wireless network. The home IWF in WSP-A serves as the anchor point for both end systems. For both end systems, data is relayed to the home IWF. The home IWF connects to an internet service provider's PPP server owned by ISP-A. Here it is assumed that both end systems have subscribed to the same ISP. If that were not the case, then the home IWF would be shown also connected to another ISP.

Within a wireless service providers network, data between base stations and the IWF is carried using the *xtunnel* protocol. Data between the IWF and the PPP server is carried using Level 2 Tunneling Protocol (L2TP). Data between the serving IWF and the home IWF is carried using the *I-xtunnel protocol.*

Always using an IWF in the home network has its advantages and disadvantages. An obvious advantage is simplicity. A disadvantage is that of always having to relay data to and from a possibly remote home IWF. The alternative is to send all the necessary information to the serving IWF so that it may connect to the end system's ISP/intranet and for the serving IWF to send accounting information in near real time back to the accounting server in the home network. This functionality is more complex to implement, but more efficient because it reduces the need to relay data over potentially long distances from the foreign network to the home network.

For example, consider a case of a user who roams from Chicago to Hong Kong. If the user's home network is in Chicago and the user registers using a wireless service provider in Hong Kong, then in the first configuration, the anchor point will be the home IWF in Chicago and all data will have to be relayed from Hong Kong to Chicago and vice versa. The home IWF in Chicago will connect to the user's ISP in Chicago. With the second configuration, the end system user will be assigned an ISP in Hong Kong. Thus, data will not always have to be relayed back and forth between Chicago and Hong Kong. In the second configuration, the serving IWF will serve as the anchor and never change for the duration of the session even if the end system moves. However, the location of the FA may change as a result of end system movement in Hong Kong.

FIG. 13 shows the second network configuration. In this figure, the home network for end system A and B is WSP-A. End system A registers from its home network, using its home IWF as an anchor point, and also connects to its ISP-A using the ISPs PPP server. End system B registers from the foreign network of WSP-B and uses a serving IWF which serves as the anchor point and connects the end system to an ISP using the ISP's PPP server. In this configuration, data for end system B does not have to be relayed from the foreign network to the home network and vice versa.

In order for this configuration to work, not only must there be roaming agreements between the home and the foreign wireless service providers, but there also must be agreements between the foreign wireless service provider and the end system's internet service provider directly or through an intermediary. In the example above, not only must the wireless service provider in Hong Kong have a business agreement with the wireless service provider in Chicago, but the WSP in

Hong Kong must have a business agreement with the user's Chicago ISP and access to the Chicago ISPs PPP server in Hong Kong or a business agreement with another ISP locally in Hong Kong who has a business agreement for roaming with the user's Chicago ISP. Additionally, the WSP in Hong Kong must be able to discover these roaming relationships dynamically in order to do user authentication and accounting and to set up the appropriate tunnels.

It is difficult for those companies who are in the Internet infrastructure business to work out suitable standards in the IETF for all of these scenarios. Thus, a preferable embodiment for the present invention is to implement the simpler, potentially less efficient configuration, where the IWF in the home network is always used as the anchor point. However, in the presence of suitable industry standardization of protocols for Internet roaming, the second configuration should be regarded as equivalent or alternative embodiment.

An end system will have to register with the wireless network before it can start PPP and send and receive data. The end system first goes through the FA discovery and registration phases. These phases authenticate and register the end system to the wireless service provider. Once these phases are over, the end system starts PPP. This includes the PPP link establishment phase, the PPP authentication phase and the PPP network control protocol phase. Once these phases are over, the end system is able to send and receive IP packets using PPP.

The following discussion assumes that the end system is roaming and registering from a foreign network. During the FA discovery phase, the end system (through its user registration agent) solicits an advertisement from the foreign agent. The user registration agent uses advertisement messages sent by a near by foreign agent to discover the identity of the FA and to register. During

this phase, the user registration agent of the end system selects the FA's care-of-address and issues a registration request to it. The FA acting as a proxy registration agent forwards the registration request to its registration server (the registration server in the foreign WSP). The registration server uses User-Name from the user registration agent's request to determine the end system's home network, and forwards the registration request for authentication to a registration server in the home network. Upon receiving the registration request relayed by the foreign registration server, the home registration server authenticates the identity of the foreign registration server and also authenticates the identity of the end system. If authentication and registration succeeds, the home registration server selects an IWF in the home network to create an *I-xtunnel* link between the home IWF and the serving IWF (in the foreign WSP). The IWF in the home network serves as the anchor point for the duration of the PPP session.

Once the mobile IP authentication and registration phases are over, the various PPP phases will be started. At the start of PPP, an L2TP connection is created between the home IWF and requested the ISP/intranet PPP server. In the PPP authentication phase, PPP passwords using PAP or CHAP are exchanged and the ISP or intranet PPP server independently authenticates the identity of the end system.

Once this succeeds, the PPP network control phase is started. In this phase, an IP address is negotiated and assigned to the end system by the PPP server and the use of TCP/IP header compression is also negotiated. When this is complete, the end system is able to send and receive IP packets using PPP to its ISP or a corporate intranet.

Note that two levels of authentication are performed. The mobile IP authentication authenticates the identity of the end system to the registration server in the home network and the identities of the foreign network and the home network to each other. To perform this function, the foreign agent forwards the end system's registration request using, for example, an IETF Radius protocol to a registration server in its local MSC in a Radius Access-Request packet. Using the end system's domain name, the foreign registration server determines the identity of the end system's home network and home registration server, and acting as a Radius proxy, encapsulates and forwards the request to the end system's home registration server. If the foreign registration server cannot determine the identity of the end system's home, it may optionally forward the Radius request to a registration server that acts like a broker (e.g. one that is owned by a consortium of wireless service providers), which can in turn proxy the Radius Access-Request to the final home registration server. If the local registration server is unable to service the registration request locally or by proxying, then it rejects the foreign agent's registration request and the foreign agent rejects the end system's registration request. Upon receiving the Radius Access-Request, the home registration server performs the necessary authentication of the identities of the foreign network and the end system. If authentication and registration succeeds, the home registration server responds with a Radius Access-Response packet to the foreign registration server which sends a response to the foreign agent so that a round trip can be completed. The registration request is rejected if the home registration server is unable to comply for any reason.

The second level of authentication verifies the identity of the end system to the intranet or ISP PPP server. PPP authentication, separate from mobility authentication allows the infrastructure equipment to be deployed and owned separately from the ISP.

FIG. 14 is a ladder diagram showing the registration sequence for a roaming end system. It is assumed that the PPP server and the home IWF are in the same server and L2TP is not required. Note the interactions with accounting servers to start accounting on behalf of the registering end system and also directory servers to determine the identity of the home registration server and to authenticate the end system's identity. More information on accounting, billing, roaming (between service providers) and settlement will be provided below.

MAC layer messages (e.g. 802.11 beacon) from the user registration agent of the end system initiate Agent Solicitation. The MAC layer messages are not shown for clarity.

In FIG. 14, the end system (mobile) initially solicits an advertisement and the foreign agent replies with an advertisement that provides the end system with information about the network to which the foreign agent belongs including a care-of-address of the foreign agent. In this case, the network is assumed to be a foreign wireless service provider. Then, a user registration agent (in the end system) incorporates the information about the foreign agent (including the care-of-address) and its network into a request and sends the request to the foreign agent. The foreign agent, as a proxy registration agent, relays the request to the foreign registration server (i.e., the registration server for the foreign wireless service provider. Then, the foreign registration server, recognizing that it is not the home directory, accesses the foreign directory server with the FDD in the foreign wireless service provider to learn how to direct the registration request to the home registration server of the wireless service provider to which the end system belongs. The foreign registration server responds with the necessary forwarding information. Then, the foreign registration server encapsulates the end system's registration request in a Radius access request and relays the encapsulated

request to the home registration server of the wireless service provider to which the end system belongs. The home registration server accesses the home directory server with the HDD of the home registration server to learn at least authentication information about the foreign service provider. Optionally, the home registration server accesses the subscriber's directory to learn detail subscriber service profile information (e.g., quality of service options subscribed to, etc.). When all parties are authenticated, the home registration server sends a start IWF request to the home IWF and PPP server. The home IWF and PPP server starts the home accounting server and then sends a start IWF response to the home registration server. The home registration server then sends a Radius access response to the foreign registration server. The foreign registration server then sends a start IWF request to the serving IWF server. The serving IWF server starts the serving accounting server and then sends a start IWF response to the foreign registration server. The foreign registration server sends a registration reply to the foreign agent, and the foreign agent relays the registration reply to the end system.

A link control protocol (LCP) configuration request is send by the end system through the foreign registration server to the home IWF and PPP server. The home IWF and PPP server sends an LCP configuration acknowledgment through the foreign registration server to the end system.

Similarly, a password authentication protocol (PAP) authentication request is sent to and acknowledged by the home IWF and PPP server. Alternatively, a challenge authentication protocol (CHAP) may be used to authenticate. Both protocols may be used to authenticate or this phase may be skipped.

Similarly, an IP configuration protocol (IPCP) configure request is sent to and acknowledged by the home IWF and PPP server.

The connection to the end system may be terminated because of any one of the following reasons.

1. *User initiated termination.* Under this scenario, the end system first terminates the PPP gracefully. This includes terminating the PPP network control protocol (IPCP) followed by terminating the PPP link protocol. Once this is done, the end system de-registers from the network followed by termination of the radio link to the access point.

2. *Loss of wireless link.* This scenario is detected by the modem and reported to the modem driver in the end system. The upper layers of the software are notified to terminate the stacks and notify the user.

3. *Loss of connection to the foreign agent.* This scenario is detected by the mobility driver in the end system. After trying to re-establish contact with a (potentially new) foreign agent and failing, the driver sends an appropriate notification up the protocol stack and also signals the modem hardware below to terminate the wireless link.

4. *Loss of connection to the IWF.* This is substantially the same as for loss of connection to the foreign agent.

5. *Termination of PPP by IWF or PPP server.* This scenario is detected by the PPP software in the end system. The end system=s PPP driver is notified of this event. It initiates de-registration from

the network followed by termination of the wireless link to the access point.

End system service configuration refers to the concept of configuring the network service for an end system based on the subscriber's service profile. The subscriber's service profile is stored in a subscriber directory. The service profile contains information to enable the software to customize wireless data service on behalf of the subscriber. This includes information to authenticate the end system, allow the end system to roam and set up connections to the end system's internet service provider. Preferably, this information also includes other parameters, like, quality of service. In addition to the subscriber directory, a home domain directory (HDD) and a foreign domain directory (FDD) are used for roaming and for authenticating the foreign and home registration servers to each other. The HDD stores information about the end system's home network and the FDD stores information about foreign networks that a subscriber may visit.

FIG. 15 shows how these directories map into the network architecture and are used during registration for an end system that is registering at home. In step 0 the end system (mobile) solicites an advertisement and the foreign agent advertises to provides the end system with information about the network to which the foreign agent belongs. In this case, the network is the home wireless service provider. In step 1, user registration agent (in the end system) incorporates the information about the foreign agent and its network into a request and sends the request to the foreign agent. In step 2, the foreign agent, as a proxy registration agent, relays the request to the home registration server. In step 3, the home registration server accesses the HDD of the home wireless service provider to learn at least authentication information. In step 4, the home registration server

accesses the subscriber directory to learn detail subscriber service profile information (e.g., quality of service options subscribed to, etc.). In step 5, the home registration server notifies the foreign agent of the access response. In steps 6 and 7, the foreign agent notifies the end system (i.e., mobile) of the registration reply.

FIG. 16 shows directory usage for an end system that is registering from a foreign network. In step 0 the end system (mobile) solicites an advertisement and the foreign agent adverstises to provides the end system with information about the network to which the foreign agent belongs. In this case, the network is a foreign wireless service provider. In step 1, user registration agent (in the end system) incorporates the information about the foreign agent and its network into a request and sends the request to the foreign agent. In step 2, the foreign agent, as a proxy registration agent, relays the request to the foreign registration server (i.e., the registration server for the foreign wireless service provider. In step 3, the foreign registration server accesses the HDD of foreign wireless service provider to learn the network to which the end system belongs. In step 4, the foreign registration server forwards the end system's request to the home registration server of the end system's home wireless service provider. In step 5, the home registration server accesses the FDD of the home registration server to learn at least authentication information about the foreign service provider. In step 6, the home registration server accesses the subscriber's directory to learn detail subscriber service profile information (e.g., quality of service options subscribed to, etc.). In step 7, the home registration server notifies the foreign registration server of the access response. In step 8, the foreign registration server forwards to the foreign agent the access response. In step 9, the foreign agent notifies the end system (i.e., mobile) of the registration reply.

Protocol handling scenarios for handling bearer data and the associated stacks for transporting bearer data to and from an end system, the protocol stacks for the cell architectures using local APs (FIG. 17) and remote APs (FIG. 18).

FIG. 17 shows the protocol stacks for handling communications between an end system (in its home network) and a home IWF for End System @ Home. FIG. 17 shows the protocol handling for a cell architecture where the access point and the wireless hub are co-located.

FIG. 18 shows the protocol handling for a cell architecture where the access point is located remotely from the wireless hub. As shown, PPP terminates in the IWF and the configuration provides direct internet access. The configuration for the case where the PPP server is separate from the IWF is described later.

In FIG. 18, PPP frames from the end system are encapsulated in RLP (radio link protocol) frames which are encapsulated at the remote access point in MAC frames for communicating with the trunk access point (i.e., an access point physically located near the wireless hub), the remote access point being coupled to the access point by, for example, a wireless trunk). The access point functions as a MAC layer bridge and relays frames from the air link to the foreign agent in the wireless hub. The foreign agent de-encapsulates the RLP frames out of the MAC frames, and using the *xtunnel* protocol, relays the RLP frames to the IWF. A similar, albeit reverse, process occurs for transmitting frames from the IWF to the end system.

If the end system moves to another foreign agent, then a new *xtunnel* will be automatically created between the new foreign agent and the IWF, so that PPP traffic continues to flow between them, without interruption.

In the remote AP cell architecture (FIG. 18) using wireless trunks between the remote AP and the trunk AP, the air link between the end system and the access point may operate at a different frequency (f1) and use a different radio technology as compared to the frequency (f2) and radio technology of the trunk.

FIG. 19 shows the protocol stacks for a roaming end system. The serving IWF uses of the *I-xtunnel* protocol between the serving IWF and home IWF. The rest of the protocol stacks remain unchanged and are not shown.

The RLP layer uses sequence numbers to drop duplicate PPP datagrams and provide in-sequence delivery of PPP datagrams between the end system and the IWF. It also provides a configurable keep-alive mechanism to monitor link connectivity between the end system and the IWF. Additionally, in an alternative embodiment, the RLP layer also provides re-transmission and flow control services in order to reduce the overall bit error rate of the link between the end system and the IWF. The RLP between the end system and the IWF is started at the beginning of the session and remains active throughout the session and even across hand-offs.

In contrast to the specification in the mobile IP RFC (RFC 2003), IP in IP encapsulation is not used for tunneling between the foreign agent and the home agent. Instead a new tunneling protocol, implemented on top of UDP is used. This tunneling protocol is a simplified version of the L2TP protocol. The reasons for this choice are as follows.

1. The encapsulation protocol specified in RFC 2003 does not provide flow control or in-sequence delivery of packets. The presently described network may need these services in the tunnel over the backhaul. Flow control may be needed to reduce the amount of re-transmissions over the air link because of packet loss due to flow control problems over the network between the base station and the MSC or because of flow control problems in the base station or the IWF.

2. By using a UDP based tunneling protocol, the implementation can be done at the user level and then put into the kernel for performance reasons, after it has been debugged.

3. Using RFC 2003, there is no easy way of creating tunnels taking into account quality of service and load balancing. In order to take QOS into account, it should be possible to set up tunnels over links that already provide the required QOS. Secondly, using RFC 2003, there is no easy way to provide load balancing to distribute bearer traffic load over multiple links between the base station and the MSC.

4. In order to implement IP in IP encapsulation as specified in RFC 2003, developers require access to IP source code. In commercial operating systems, source code for the TCP/IP stack is generally proprietary to other equipment manufacturers. Purchasing the TCP/IP stack from a vendor and making changes to the IP layer to support mobile IP tunneling would require a developer to continue supporting a variant version of the TCP/IP stack. This adds cost and risk.

While it is noted that the tunneling protocol between the base station and the IWF is non-standard and that the wireless service provider will not be able to mix and match equipment from different vendors, the use of a non-standard tunneling protocol within a single wireless service provider network is transparent to end systems and equipment from other vendors.

The new tunneling protocol is based on L2TP. By itself, L2TP is a heavyweight tunneling protocol so that L2TP has a lot of overhead associated with tunnel creation and authentication. The new tunneling protocol of the present invention has less overhead. The new xtunnel protocol has the following features.

1. The *xtunnel* creation adds vendor specific extensions to Radius Access Request and Radius Access Response messages between the base station and the registration server. These extensions negotiate tunnel parameters and to create the tunnel.

2. The registration server is able to delegate the actual work of tunneling and relaying packets to a different IP address, and therefore, to a different server in the MSC. This permits the registration server to do load balancing across multiple IWF servers and to provide different QOS to various users.

3. The *xtunnel* protocol supports in-band control messages for tunnel management. These messages include echo request/response to test tunnel connectivity, disconnect request/response/notify to disconnect the tunnel and error notify for error notifications. These messages are sent over the tunneling media, for example, UDP/IP.

4. The *xtunnel* protocol sends payload data over the tunneling media, for example, UDP/IP. The *xtunnel* protocol supports flow control and in-sequence packet delivery.

5. The *xtunnel* protocol may be implemented over media other than UDP/IP for quality of service.

The network supports direct internet connectivity by terminating the PPP in the home IWF and routing IP packets from the IWF to the internet via a router using standard IP routing techniques. Preferably, the IWF runs RIP, and the router also runs RIP and possibly other routing protocols like OSPF.

The network supports a first configuration for a wireless service provider who is also an internet service provider. In this configuration, the home IWF in the MSC also functions as a PPP server. This IWF also runs internet routing protocols like RIP and uses a router to connect to the internet service provider=s backbone network.

The network supports a second configuration for a wireless service provider who wishes to allow end systems to connect to one or more internet service providers, either because the WSP itself is not ISPs, or because the WSP has agreements with other ISPs to provide access to end users. For example, a wireless service provider may elect to offer network access to an end user and may have an agreement with a 3rd party ISP to allow the user who also has an account with the 3rd party ISP to access the ISP from the WSP network. In this configuration, the PPP server does not run in the home IWF installed at the MSC. Instead, a tunneling protocol like L2TP (Layer Two Tunneling Protocol) is used to tunnel back to the ISP's PPP server. FIG. 10 shows the protocol stacks for this

configuration for an end system that is at home.

The location of the home IWF and the ISP PPP server remains fixed throughout the PPP session. Also, the L2TP tunnel between the IWF and the ISP's PPP server remains up throughout the PPP session. The physical link between the IWF and the PPP server is via a router using a dedicated T1 or T3 or frame relay or ATM network. The actual nature of the physical link is not important from the point of view of the architecture.

This configuration also supports intranet access. For intranet access, the PPP server resides in the corporate intranet and the home IWF uses L2TP to tunnel to it.

For a roaming end system, the protocol handling for intranet or ISP access is as shown in FIG. 20 with the difference that the roaming end system uses a serving IWF to connect to its home IWF. The protocol handling between a serving IWF and a home IWF has been described earlier.

FIG. 21 shows the protocol stacks used during the registration phase (end system registration) for a local AP cell architecture. The stack for a remote AP cell architecture is very similar.

The scenario shown above is for a roaming end system. For an end system at home, there is no foreign registration server in the registration path.

Note the mobility agent in the end system. The mobility agent in the end system and foreign agent in the wireless hub are conceptually similar to the mobile IP RFC 2002. The mobility agent handles network errors using time-outs and re-

trys. Unlike the known protocol stacks for bearer data, RLP is not used. The foreign agent and the registration servers use Radius over UDP/IP to communicate with each other for registering the end system.

Several aspects of security must be considered. The first, authenticating the identities of the end system and the foreign/home networks during the wireless registration phase. Second, authenticating the identity of the end system with its PPP server during the PPP authentication phase. Third, authentication for storing accounting data, for billing and for updating home domain information. Fourth, encryption of bearer traffic transmitted to and from the end system. Fifth, encryption for exchanging billing information across service provider boundaries.

Shared secrets are used to authenticate the identity of end systems with their home networks and the identity of the home and foreign networks with each other during wireless registration.

End system authentication uses a 128-bit shared secret to create an authenticator for its registration request. The authenticator is created using the known MD5 message digest algorithm as described in the mobile IP RFC 2002. The shared secret is not sent in the registration request by the end system. Only the authenticator is sent. On receiving the registration request from the end system, the home registration server re-computes the authenticator over the registration request data using the shared secret. If the computed authenticator value matches the authenticator value sent by the end system, the home registration server allows the registration process to proceed. If the values do not match, the home registration server logs the event, generates a security violation alarm and a nak (i.e., a negative acknowledgment) to the request.

In the registration reply, the home registration server does the same - that is to say, uses the shared secret to create an authenticator for the registration reply that it sends to the end system. Upon receiving the reply, the end system re-computes the authenticator using the shared secret. If the computed value does not match the authenticator value sent by the home registration server in the reply, the end system discards the reply and tries again.

These network security concepts are similar to the concepts defined in mobile IP RFC 2002. According to the RFC, a mobility security association exist between each end system and its home network. Each mobility security association defines a collection of security contexts. Each security context defines an authentication algorithm, a mode, a secret (shared or public-private), style of replay protection and the type of encryption to use. In the context of the present network, the end system's User-Name (in lieu of the home address) is used to identify the mobility security association between the end system and its home network. Another parameter, called the security parameter index (SPI), is used to select a security context within the mobility security association. In a basic embodiment of the invention, only the default mobile IP authentication algorithm (keyed-MD5) and the default mode ("prefix+suffix") are supported with 128-bit shared secrets. Network users are allowed to define multiple shared secrets with their home networks. The mechanism for creating security contexts for end users, assigning an SPI to each security context and for setting the contents of the security context (which includes the shared secret) and for modifying their contents are described below. During registration, a 128 bit message digest is computed by the end system in prefix+suffix mode using the MD5 algorithm. The shared secret is used as the prefix and the suffix for the data to be protected in the registration request. The authenticator thus computed, along with the SPI and

the User-Name are transmitted in the registration request by the end system. Upon receiving the end system's registration request, the foreign registration server relays the request along with the authenticator and the SPI, unchanged to the home registration server. Upon receiving the registration request directly from the end system or indirectly via a foreign registration server, the home registration server uses the SPI and the User-Name to select the security context. The home server re-computes the authenticator using the shared secret. If the computed authenticator value matches the value of the authenticator sent in the request by the end system, the user's identity will have been successfully authenticated. Otherwise, the home registration server naks (negatively acknowledges) the registration request sent by the end system.

The registration reply sent by the home registration server to the end system is also authenticated using the mobile IP algorithm described above. The SPI and the computed authenticator value is transmitted in the registration reply message by the home server to the end system. Upon receiving the reply, the end system re-computes the authenticator, and if the computed value does not match the transmitted value, it will discard the reply and retry.

The user's end system has to be configured with the shared secret and SPIs for all security contexts that the user shares with its registration server(s). This configuration information is preferably stored in a Win 95 registry for Windows 95 based end systems. During registration, this information is accessed and used for authentication purposes.

In the network, Radius protocols are used by foreign agent FA to register the end system and to configure the *xtunnel* between the wireless hub and the home and serving IWFs on behalf of the end system. On receiving a registration request from the end system, the FA creates a Radius Access-Request packet, stores its own attributes into the packet, copies the end system's registration request attributes unchanged into this packet and sends the combined request to the registration server in the MSC.

Radius authentication requires that the Radius client (in this case, the FA in the base station) and the Radius server (in this case, the registration server in the MSC) share a secret for authentication purposes. This shared secret is also used to encrypt any private information communicated between the Radius client and the Radius server. The shared secret is a configurable parameter. The network follows the recommendations in the Radius RFC and uses the shared secret and the MD5 algorithm for authentication and for encryption, where encryption is needed. The Radius Access Request packet sent by the FA contains a Radius User-Name attribute (which is provided by the end system) and a Radius User-Password attribute. The value of the User Password attribute is also a configurable value and encrypted in the way recommended by the Radius protocol. Other network specific attributes, which are non-standard attributes from the point of view of the Radius RFC standards, are encoded as vendor specific Radius attributes and sent in the Access-Request packet.

The following attributes are sent by the FA to its registration server in the Radius Access-Request packet.

1. *User-Name Attribute.* This is the end system's user-name as supplied by the end system in its registration request.

2. *User-Password Attribute.* This user password is supplied by the base station/wireless hub on behalf of the user. It is encoded as described in the Radius EFC using the secret shared between the base station and its registration server.

3. *NAS-Port.* This is the port on the base station.

4. *NAS-IP-Address.* This is the IP address of the base station.

5. *Service-Type.* This is framed service.

6. *Framed Protocol.* This is a PPP protocol.

7. *Xtunnel Protocol Parameters*. These parameters are sent by the base station to specify the parameters necessary to set up the *xtunnel* protocol on behalf of the end system. This is a vendor-specific attribute.

8. *AP-IP-Address*. This is the IP address of the AP through which the user is registering. This is a vendor-specific attribute.

9. *AP-MAC-Address*. This is the MAC address of the AP through which the user is registering. This is a vendor-specific attribute.

10. *End system's Registration Request*. The registration request from the end system is copied unchanged into this vendor specific attribute.

The following attributes are sent to the FA from the registration server in the Radius Access-Response packet.

1. *Service Type*. This is a framed service.

2. *Framed-Protocol*. This is a PPP.

3. *Xtunnel Protocol Parameters*. These parameters are sent by the registration server to specify the parameters necessary to set up the *xtunnel* protocol on behalf of the end system. This is a vendor-specific attribute.

4. *Home Registration Server's Registration Reply*. This attribute is sent to the FA from the home registration server. The FA relays this attribute unchanged to the end system in a registration reply packet. If there is a foreign registration server in the path, this attribute is relayed by it to the FA unchanged. It is coded as a vendor-specific attribute.

To provide service to roaming end systems, the foreign network and the home network are authenticated to each other for accounting and billing purposes using the Radius protocol for authentication and configuration. This authentication is performed at the time of end system registration. As described earlier, when the registration server in the foreign network receives a registration request from an end system (encapsulated as a vendor specific attribute in a Radius-Access Request packet by the FA), it uses the end system=s User-Name to determine the identity of the end system=s home registration server by consulting its home domain directory HDD. The following information is stored in home domain directory HDD and accessed by the foreign registration server in order to forward the end system's registration request.

1. *Home Registration Server IP Address.* This is the IP address of the home registration server to forward the registration request.

2. *Foreign Registration Server Machine Id.* This is the machine ID of the foreign registration server in SMTP (simplified mail transfer protocol) format (e.g., machine@fqdn where machine is the name of the foreign registration server machine and fqdn is the fully qualified domain name of the foreign registration server's domain).

3. *Tunneling Protocol Parameters.* These are parameters for configuring the tunnel between the serving IWF and the home IWF on behalf of the end system. These include the tunneling protocol to be used between them and the parameters for configuring the tunnel.

4. *Shared Secret.* This is the shared secret to be used for uthentication between the foreign registration server and the home registration server. This secret is used for computing the Radius User-Password attribute in the Radius packet sent by the foreign registration server to the home registration server. It is defined between the two wireless service providers.

5. *User-Password*. This is the user password to be used on behalf of the roaming end system. This user password is defined between the two wireless service providers. This password is encrypted using the shared secret as described in the Radius RFC.

6. *Accounting Parameters*. These are parameters for configuring accounting on behalf of the end system that is registering. These parameters are sent by the registration server to its IWF for configuring accounting on behalf of the end system.

Using this information, the foreign registration server creates a Radius Access-Request, adds its own registration and authentication information into the Radius Access-Request, copies the registration information sent by the end system unchanged into the Radius Access-Request and sends the combined request to the home registration server.

Upon receiving the Radius-Access Request from the foreign registration server (for a roaming end system) or directly from the FA (for an end system at home), the home registration server consults its own directory server for the shared secrets to verify the identity of the end system and the identity of the foreign registration server in a roaming scenario by re-computing authenticators.

After processing the request successfully, the home registration server creates a Radius Access-Accept response packet and sends it to the foreign registration server if the end system is roaming, or directly to the FA from which it received the Radius Access-Request. The response contains the registration reply attribute that the FA relays to the end system.

If the request can not be processed successfully, the home registration server creates a Radius Access-Reject response packet and sends it to the foreign registration server if the end system is roaming, or directly to the FA from which it received the Radius Access-Request. The response contains the registration reply attribute that the FA will relays to the end system.

In a roaming scenario, the response from the home registration server is received by the foreign registration server. It is authenticated by the foreign registration server using the shared secret. After authenticating, the foreign registration server processes the response, and in turn, it generates a Radius response packet (Accept or Reject) to send to the FA. The foreign registration server copies the registration reply attribute from the home registration server's Radius response packet, unchanged, into its Radius response packet.

When the FA receives the Radius Access-Response or Radius Access-Reject response packet, it creates a registration reply packet using the registration reply attributes from the Radius response, and sends the reply to the end system, thus completing the round trip registration sequence.

Mobile IP standards specifies that replay protection for registrations are implemented using time stamps, or optionally, using nonces. However, since replay protection using time stamps requires adequately synchronized time-of-day clocks between the corresponding nodes, the present invention implements replay protection during registration using nonces even though replay protection using time stamps is mandatory in the Mobile IP standards and the use nonces is optional. However, replay protection using time stamps as an alternative embodiment is envisioned.

The style of replay protection used between nodes is stored in the security context in addition to the authentication context, mode, secret and type of encryption.

The network supports the use of PPP PAP (password authentication) and CHAP (challenge authenticated password) between the end system and its PPP server. This is done independently of the mobile IP and Radius based authentication mechanisms described earlier. This allows a private intranet or an ISP to independently verify the identity of the user.

Authentication for accounting and directory services is described below with respect to accounting security. Access to directory servers from network equipment in the same MSC need not be authenticated.

The network supports encryption of bearer data sent between the end system and the home IWF. End systems negotiate encryption to be on or off by selecting the appropriate security context. Upon receiving the registration request, the home registration server grants the end system's request for encryption based upon the security context. In addition to storing the authentication algorithm, mode, shared secret and style of replay protection, the security context is also used to specify the style of encryption algorithm to use. If encryption is negotiated between the end system and the home agent, then the complete PPP frame is so encrypted before encapsulation in RLP.

The IWF, the accounting server and the billing system are part of the same trusted domain in the MSC. These entities are either connected on the same LAN or part of a trusted intranet owned and operated by the wireless service provider. Transfer of accounting statistics between the IWF and the accounting server and between the accounting server and the customer's billing system need not be encrypted.

The network makes it more difficult to monitor the location of the end system because it appears that all PPP frames going to and from the end system go through the home IWF regardless of the actual location of the end system device.

Accounting data is collected by the serving IWF and the home IWF in the network. Accounting data collected by the serving IWF is sent to an accounting server in the serving IWF's MSC. Accounting data collected by the home IWF is sent to an accounting server in the home IWF's MSC. The accounting data collected by the serving IWF is used by the foreign wireless service provider for auditing and for settlement of bills across wireless service provider boundaries (to support roaming and mobility). The accounting data collected by the home IWF is used for billing the end user and also for settlement across wireless service provider boundaries to handle roaming and mobility.

Since all data traffic flows through the home IWF, regardless of the end system's location and the foreign agent's location, the home IWF has all the information to generate bills for the customer and also settlement information for the use of foreign networks.

The serving IWF and the home IWF preferably use the Radius accounting protocol for sending accounting records for registered end systems. The Radius accounting protocol is as documented in a draft IETF RFC. For the present invention, the protocol has to be extended by adding vendor specific attributes for the network and by adding check-pointing to the Radius Accounting protocol. Check-pointing in this context refers to the periodic updating of accounting data to minimize risk of loss of accounting records.

The Radius accounting protocol runs over UDP/IP and uses re-trys based on acknowledgment and time outs. The Radius accounting client (serving IWFs or home IWFs) send UDP accounting request packets to their accounting servers which send acknowledgments back to the accounting clients.

In the network, the accounting clients (serving IWF and the home IWF) emit an accounting start indication at the start of the user's session and an accounting stop indication at the end of the user's session. In the middle of the session, the accounting clients emit accounting checkpoint indications. In contrast, the Radius accounting RFC does not specify an accounting checkpoint indication. The software of the present invention creates a vendor specific accounting attribute for this purpose. This accounting attribute is present in all Radius Accounting-Request packets which have Acct-Status-Type of Start (accounting start indications). The value of this attribute is used to convey to the accounting server whether the accounting record is a check-pointing record or not. Check-pointing accounting reports have a time attribute and contain cumulative accounting data from the start of the session. The frequency of transmitting check-point packets is configurable in the present invention.

The serving IWF and the home IWF are configured by their respective registration servers for connecting to their accounting servers during the

registration phase. The configurable accounting parameters include the IP address and UDP port of the accounting server, the frequency of check-pointing, the session/multi-session id and the shared secret to be used between the accounting client and the accounting server.

The network records the following accounting attributes for each registered end system. These accounting attributes are reported in Radius accounting packets at the start of the session, at the end of the session and in the middle (check-point) by accounting clients to their accounting servers.

1. *User Name*. This is like the Radius User-Name attribute discussed above. This attribute is used to identify the user and is present in all accounting reports. The format is "user@domain" where domain is the fully qualified domain name of the user's home.

2. *NAS IP Address*. This is like the Radius NAS-IP-Address attribute discussed above. This attribute is used to identify the IP address of the machine running the home IWF or the serving IWF.

3. *Radio Port*. This attribute identifies the radio port on the access point providing service to the user. This attribute is encoded as a vendor specific attribute.

4. *Access Point IP Address*. This attribute identifies the IP address of the access point providing service to the user. This attribute is encoded as a vendor specific attribute.

5. *Service Type*. This is like the Radius Service-Type attribute described above. The value of this attribute is Framed.

6. *Framed Protocol*. This is like the Radius Framed Protocol attribute described above. The value of this attribute is set to indicate PPP.

7. *Accounting Status Type*. This is like the Radius Acct-Status-Type attribute described above. The value of this attribute may be Start to

mark the start of a user's session with the Radius client and Stop to mark the end of the user's session with the Radius client. For accounting clients, the Acct-Status-Type/Start attribute is generated when the end system registers. The Acct-Status-type/Stop attribute is generated when the end system de-registers for any reason. For checkpoints, the value of this attribute is also Start and the *Accounting Checkpoint* attribute is also present.

8. *Accounting Session Id.* This is like the Radius Acct-Session-Id described above. In a roaming scenario, this session id is assigned by the foreign registration server when the end system issues a registration request. It is communicated to the home registration server by the foreign registration server during the registration sequence. The home network and the foreign network both know the Acct-Session-Id attribute and are able to emit this attribute while sending accounting records to their respective accounting servers. In a "end system-at-home" scenario, this attribute is generated by the home registration server. The registration server communicates the value of this attribute to the IWF which emits it in all accounting records.

9. *Accounting Multi-Session Id.* This is like the Radius Acct-Multi-Session-Id discussed above. This id is assigned by the home registration server when a registration request is received from a FA directly or via a foreign registration server on behalf of an end system. It is communicated to the foreign registration server by the home registration server in the registration reply message. The registration server(s) communicates the value of this attribute to the IWF(s) which emit it in all accounting records.

With true mobility added to the architecture, the id is used to relate together the accounting records from different IWFs for the same end system if the end system moves from one IWF to another. For hand-offs across IWF

boundaries, the Acct-Session-Id is different for accounting records emanating from different IWFs. However, the Acct-Multi-Session-Id attribute is the same for accounting records emitted by all IWFs that have provided service to the user. Since the session id and the multi-session id are known to both the foreign network and the home network, they are able to emit these attributes in accounting reports to their respective accounting servers. With the session id and the multi-session id, billing systems are able to correlate accounting records across IWF boundaries in the same wireless service provider and even across wireless service provider boundaries.

1. *Accounting Delay Time.* See Radius Acct-Delay-Time attribute.

2. *Accounting Input Octets.* See Radius Acct-Input-Octets. This attribute is used to keep track of the number of octets sent by the end system (input to the network from the end system). This count is used to track the PPP frames only. The air link overhead, or any overhead imposed by RLP, etc. and is not counted.

3. *Accounting Output Octets.* See Radius Acct Output-Octets. This attribute is used to keep track of the number of octets sent to the end system (output from the network to the end system). This count is used to track the PPP frames only. The air link overhead, or any overhead imposed by RLP, etc. and is not counted.

4. *Accounting Authentic.* See Radius Acct-Authentic attribute. The value of this attribute is Local or Remote depending on whether the serving IWF or the home IWF generates the accounting record.

5. *Accounting Session Time.* See Radius Acct-Session-Time attribute. This attribute indicates the amount of time that the user has been receiving service. If sent by the serving IWF, this attribute tracks the amount of time that the user has been receiving service from that serving IWF. If sent by the home IWF, this attribute tracks the

amount of time that the user has been receiving service from the home IWF.

6. *Accounting Input Packets*. See Radius Acct-Input-Packets attribute. This attribute indicates the number of packets received from the end system. For a serving IWF, this attribute tracks the number of PPP frames input into the serving IWF from an end system. For a home IWF, this attribute tracks the number of PPP frames input into the home IWF from an end system.

7. *Accounting Output Packets*. See Radius Acct-Output-Packets attribute. This attribute indicates the number of packets sent to the end system. For a serving IWF, this attribute tracks the number of PPP frames output by the serving IWF to the end system. For a home IWF, this attribute tracks the number of PPP frames sent to the end system from the home IWF.

8. *Accounting Terminate Cause*. See Radius Acct-Terminate-Cause attribute. This attribute indicates the reason why a user session was terminated. In addition, a specific cause code is also present to provide additional details. This attribute is only present in accounting reports at the end of the session.

9. *Network Accounting Terminate Cause*. This attribute indicates a detailed reason for terminating a session. This specific attribute is encoded as a vendor specific attribute and is only reported in a Radius Accounting attribute at the end of session. The standard Radius attribute Acct-Terminate-Cause is also present. This attribute provides specific cause codes, not covered by the Acct-Terminate-Cause attribute.

10. *Network Air link Access Protocol*. This attribute indicates the air link access protocol used by the end system. This attribute is encoded as a vendor specific attribute.

11. *Network Backhaul Access Protocol.* This attribute indicates the backhaul access protocol used by the access point to ferry data to and from the end system. This attribute is encoded as a vendor specific attribute.

12. *Network Agent Machine Name.* This attribute is the fully qualified domain name of the machine running the home IWF or the serving IWF. This specific attribute is encoded in vendor specific format.

13. *Network Accounting Check-point.* Since the Radius accounting RFC does not define a check-point packet, the present network embodiment uses a Radius accounting start packet with this attribute to mark a check-point. The absence of a check-point attribute means a conventional accounting start packet. The presence of this attribute in a accounting start packet means a accounting check-point packet. Accounting stop packets do not have this attribute.

In the preferred embodiment, every accounting packet and the corresponding reply must be authenticated using MD5 and a shared secret. The IWFs are configured with a shared secret that are used by them for authentication during communication with their Radius accounting server. The shared secrets used by the IWFs for communicating with accounting servers are stored in the home/foreign domain directory located in the MSC. The shared secrets for accounting security are communicated to the IWFs by their registration servers during the end system registration sequence.

The accounting server software runs in a computer located in the MSC. The role of the accounting server in the system is to collect raw accounting data from the network elements (the home and the serving IWFs), process the data and store it for transfer to the wireless service provider's billing system. The accounting server does not include a billing system. Instead, it includes support for an automatic or manual accounting data transfer mechanism. Using the automatic accounting data transfer mechanism, the accounting server transfers accounting records in AMA billing format to the customer's billing system over a

TCP/IP transport. For this purpose, the system defines AMA billing record formats for packet data. Using the manual transfer mechanism, customers are able to build a tape to transfer accounting records to their billing system. In order to build the tape to their specifications, customers are provided with information to access accounting records so that they may process them before writing them to tape.

In FIG. 22, the raw accounting data received by the accounting server from the home or serving IWFs are processed and stored by the accounting server. The processing done by the accounting server includes filtering, compression and correlation of the raw accounting data received from the IWF. A high availability file server using dual active/standby processors and hot swappable RAID disks is used for buffering the accounting data while it is transiting through the accounting server.

The accounting server delays processing of the raw accounting data until an end system has terminated its mobile IP session. When an end system terminates its session, the accounting server processes the raw accounting data that it has collected for the session and stores an accounting summary record in a SQL database. The accounting summary record stored in the SQL data base points to an ASN.1 encoded file. This file contains detailed accounting information about the end system's session. The data stored in the accounting server is then transferred by the billing data transfer agent to the customer's billing system. Alternatively, the wireless service provider may transfer the accounting data from the SQL database and/or the ASN.1 encoded file to the billing system via a tape. The data base scheme and the format of the ASN.1 encoded file are documented and made available to customers for this purpose. If the volume of processed accounting data stored in the accounting system exceeds a high water mark, the accounting server generates an NMS alarm. This alarm is cleared when the volume of data stored in the accounting server falls below a low water mark. The high and low water marks for generating and clearing the alarm are configurable. The accounting server also generates an NMS alarm if the age of the stored

accounting data exceeds a configurable threshold. Conversely, the alarm is cleared, when the age of the accounting data falls below the threshold.

The subscriber directory is used to store information about subscribers and is located in the home network. The home registration server consults this directory during the registration phase to authenticate and register an end system. For each subscriber, the subscriber directory stores the following information.

1. *User Name.* This field in the subscriber record will be in SMTP format (e.g., *user@fqdn)* where the *user* sub-field will identify the subscriber in his or her wireless home domain and the *fqdn* sub-field will identify the wireless home domain of the subscriber. This field is sent by the end system in its registration request during the registration phase. This field is assigned by the wireless service provider to the subscriber at the time of subscription to the network service. This field is different than the user name field used in PPP.

2. *Mobility Security Association.* This field in the subscriber record contains the mobility security association between the subscriber and his or her home network. As described above, a mobility security association exists between each subscriber and its home registration server. The mobility security association defines a collection of security contexts. Each security context defines an authentication algorithm, an authentication mode, a shared secret, style of replay protection and the type of encryption (including no encryption) to use between the end system and its home server. During registration, the home registration server retrieves information about the subscriber's security context from the subscriber directory using the *User-Name* and the *security parameter index (SPI)* supplied by the end system in its registration request. The information in the security context is used for enforcing authentication, encryption and replay protection during

the session. The mobility security association is created by the wireless service provider at the time of subscription. It is up to the wireless service provider to permit the subscriber to modify this association either by calling up a customer service representative or by letting subscribers access to a secure Web site. The Web site software will export web pages which the wireless service provider may make accessible to subscribers from a secure web server. In this way, subscribers are able to view/modify the contents of the mobility security association in addition to other subscriber information that the service provider may make accessible.

3. *Modem MAC Address*. This field contains the MAC address of the modem owned by the subscriber. In addition to the shared secret, this field is used during registration to authenticate the user. It is possible to turn off MAC address based authentication on a per user basis. The MAC address is communicated to the home registration server during registration.

4. *Enable MAC Address Authentication*. This field is used to determine if MAC address based authentication is *enabled* or *disabled*. If *enabled*, the home registration server checks the MAC address of the registering end system against this field to validate the end system's identity. If *disabled*, then no checking is done.

5. *Roaming Enabled Flag*. If this field is set to *enabled*, then the end system is allowed to roam to foreign networks. If this field is *disabled*, then the end system is not permitted to roam to foreign networks.

6. *Roaming Domain List*. This field is meaningful only if the *Roaming Enabled Flag* is set to *enabled*. This field contains a list of foreign domains that the end system is allowed to roam to. When the contents of this list is null and the *Roaming Enabled Flag* is set to *enabled*, the end system is allowed to roam freely.

7. *Service Enable/Disable Flag*. This field may be set to *disabled* by the system administrator to disable service to a subscriber. If this field is disabled, then the subscriber is be permitted to register for service. If the subscriber is registered and the value of this field is set to disabled, then the subscriber's end system is immediately disconnected by the network.

8. *Internet Service Provider Association*. This field contains information about the subscriber's internet service provider. This information is used by the IWF during the PPP registration phase to perform authentication with the internet service provider on behalf of the end system and also to create a L2TP tunnel between the IWF and the internet service provider's PPP server. This field contains the identity of the subscriber's ISP. The IWF uses this information to access the ISP directory for performing authentication and setting up the L2TP tunnel on behalf of the end system.

9. *Subscriber's Name & Address Information*. This field contains the subscriber's name, address, phone, fax, e-mail address, etc.

The home domain directory (HDD) is used by the registration server to retrieve parameters about the end system to complete registration on behalf of the end system. Using this information, the registration server determines if the end system is registering at home or if the end system is a roaming end system. In the former case, the registration server assumes the role of a home registration server and proceed with end system registration. In the latter case, the registration server assumes the role of a foreign registration server and, acting as a Radius proxy, it forwards the request to the real home registration server whose identity it gets from this directory. For roaming end system, the parameters stored in the HDD include the IP address of the home registration server, the home-foreign shared secret, the home-serving IWF tunnel configuration etc. The HDD is located in the MSC.

The following information is stored in the HDD.

1. *Home Domain Name.* This field is used as the key to search the HDD for an entry that matches the fully qualified home domain name provided by the end system in its registration request.

2. *Proxy Registration Request.* This field is used by the registration server to determine if it should act as a foreign registration server and proxy the end system's registration request to the real home registration server.

3. *Home Registration Server DNS Name.* If the *proxy registration request* flag is TRUE, this field is used to access the DNS name of the real home registration server. Otherwise, this field is ignored. The DNS name is translated to an IP address by the foreign registration server. The foreign registration server uses the IP address to relay the end system's registration request.

4. *Foreign Domain Name.* If the *proxy registration request* flag is TRUE, this field is used to identify the foreign domain name to the end system's home registration server. Otherwise, this field is ignored. The foreign registration server uses this information to create the foreign server machine id in SMTP format, for example, *machine@fqdn*. This machine id is sent to the home registration server by the foreign registration server in the Radius-Access Request.

5. *Shared Secret.* If the *proxy registration request* flag is TRUE, the shared secret is used between the foreign and home registration servers to authenticate their identity with each other. Otherwise this field is ignored.

6. *Tunneling Protocol Parameters.* This field is used to store parameters to configure the tunnels to provide service to the end system. For an end system at home, this includes information on

tunnel parameters between the base station and the home IWF and from the home IWF to the PPP server. For a roaming end system, this includes tunneling parameters from the base station to the serving IWF and from the serving IWF to the home IWF. At a minimum, for each tunnel, this field contains the type of tunneling protocol to use and any tunneling protocol specific parameters. For example, this field may contain the identifier for the tunneling protocol L2TP and any additional parameters required to configure the L2TP tunnel between the IWF and its peer.

7. *Accounting Server Association.* This field is used to store information needed by the IWF to generate accounting data on behalf of the end system. It contains the name of the accounting protocol (e.g. RADIUS), the DNS name of the accounting server and additional parameters specific to the accounting protocol like the UDP port number, the shared secret that the IWF must use in the Radius Accounting protocol, the frequency of check-pointing, the seed for creating the session/multi-session id, etc. The accounting server's DNS name is translated to the accounting server's IP address, which is sent to the IWF.

For wireless service providers that have roaming agreements with each other, the HDD is used for authentication and to complete the registration process. If an end system roams from its home network to a foreign network, the foreign registration server in that network consults the HDD in its MSC to get information about the visiting end system's home registration and to authenticate the home network before it provides service to the visiting end system.

The software for home domain directory management preferably provides a graphical user interface (GUI) based HDD management interface for system administrators. Using this GUI, system administrators are able to view and update entries in the HDD. This GUI is not intended for use by foreign wireless network service providers to perform remote updates based on roaming agreements. It is only

intended for use by trusted personnel of the home wireless service provider operating behind fire walls.

The foreign domain directory (FDD) provides functionality that is the reverse of the home domain directory. The FDD is used by the home registration server to retrieve parameters about the foreign registration server and the foreign network in order to authenticate the foreign network and create a tunnel between a serving IWF and a home IWF. These parameters include the home-foreign shared secret, the home IWF-serving IWF tunnel configuration, etc. The FDD is preferably located in the home registration server's MSC. The FDD is used by home registration servers for registering roaming end systems.

The following information will be stored in the FDD.

1. *Foreign Domain Name.* This field is used as the key to search the FDD for an entry that matches the fully qualified domain name of the foreign registration server relaying the registration request.

2. *Shared Secret.* This is the shared secret used between the foreign and home registration servers to authenticate their identity mutually with each other.

3. *Home IWF-Serving IWF Tunneling Protocol Parameters.* This field is used to store parameters to configure the tunnel between the home IWF and the serving IWF. At a minimum, this field contains the type of tunneling protocol to use and any tunneling protocol specific parameters. For example, this field may contain the identifier for the tunneling protocol L2TP and any additional parameters required to configure the L2TP tunnel between the serving IWF and the home IWF.

4. *Accounting Server Association.* This field is used to store information needed by the home IWF to generate accounting data on behalf of the end system. It contains the name of the accounting protocol (e.g. RADIUS), the DNS name of the accounting server and additional

parameters specific to the accounting protocol like the UDP port number, the shared secret that the IWF must use in the Radius Accounting protocol, the frequency of check-pointing, the seed for creating the session/multi-session id, etc. The accounting server's DNS name is translated to the accounting server's IP address, which is sent to the foreign agent.

For wireless service providers that have roaming agreements with each other, the FDD is used to do authentication and complete the registration process. If an end system roams from its home network to a foreign network, the registration server in the home network consults the FDD in its MSC to get information and authenticate the foreign network providing service to the end system.

The foreign domain directory management software provides a graphical user interface (GUI) based FDD management interface for system administrators. Using this GUI, system administrators are able to view and update entries in the FDD. This GUI is not intended for use by foreign wireless network service providers to perform remote updates based on roaming agreements. It is only intended for use by trusted personnel of the home wireless service provider operating behind firewalls.

The internet service provider directory (ISPD) is used by the home IWF to manage connectivity with ISPs that have service agreements with the wireless service provider so that subscribers may access their ISPs using the network. For each subscriber, the subscriber directory has an entry for the subscriber's ISP. This field points to an entry in the ISPD. The home IWF uses this information to set up the connection to the ISP on behalf of the subscriber.

The network architecture supports roaming. In order for roaming to work between wireless service providers, the architecture must support the setting up of roaming agreements between wireless service providers. This implies two things: (1) updating system directories across wireless service providers and (2) settlement of bills between service providers.

In order to allow subscribers access to internet service providers, the architecture supports roaming agreements with internet service providers. This implies that the architecture must be able to send data to and receive data from ISP PPP servers (i.e., that support industry standard protocols like PPP, L2TP and Radius). It also implies that the architecture handles directory updates for ISP access and settlement of bills with ISPs.

When roaming agreements are established between two wireless service providers, both providers have to update their home and foreign domain directories in order to support authentication and registration functions for end systems visiting their networks from the other network. At a minimum, the architecture of the present embodiment supports manual directory updates. When a roaming agreement is established between two wireless service providers, then the two parties to the agreement exchange information for populating their home and foreign domain directories. The actual updates of the directories is done manually by the personnel of the respective service providers. If later, the information in the home and foreign domain directories needs to be updated, the two parties to the agreement exchange the updated information and then manually apply their updates to the directories.

In an alternative embodiment, the directory management software incorporates developing standards in the IETF to enable roaming between internet service providers and to enable ISPs to automatically manage and discover roaming relationships. This makes manual directory management no longer necessary. The network system automatically propagates roaming relationships, and discovers them, to authenticate and register visiting end systems.

At a minimum, the network architecture just processes and stores the accounting data and makes the data available to the wireless service provider's billing system. It is up to the billing system to handle settlement of bills for roaming.

In an alternative embodiment, developing standards in the IETF to handle distribution of accounting records between internet service providers are incorporated into the network architecture to enable ISPs to do billing settlement for roaming end systems.

The system software supports access to ISPs and private intranets by supporting L2TP between the home IWF and the ISPs or intranet PPP server. The internet service provider directory contains information useful to the IWF for creating these tunnels. As access agreements between the wireless service provider and internet service providers are put in place, this directory is updated manually by the wireless service provider's personnel. Automatic updates and discovery of access relationships between the wireless service provider and internet service providers are presently contemplated and implemented as the internet standards evolve. While accessing an internet service provider, the subscriber receives two bills - one from the wireless service provider for the use of the wireless network and the second from the internet service provider. Although common billing that combines both types of charges is not handled by the minimum embodiment software, it is contemplated that the software will take advantage of internet standards for billing settlement as they evolve so that subscribers may receive a common bill based on roaming agreements between the ISP and wireless service providers.

The system includes a element management system for managing the network elements. From the element manager, system administrators perform configuration, performance and fault/alarm management functions. The element management applications run on top of a web browser. Using a web browser, system administrators manage the network from anywhere that they have TCP/IP access. The element manager also performs an agent role for a higher level manager. In this role it exports an SNMP MIB for alarm and fault monitoring.

A higher level SNMP manager is notified of alarm conditions via SNMP traps. The higher level SNMP manager periodically polls the element manager=s MIB for the health and status of the network. System management personnel at the higher level manager are able to view an icon representation of the network and its current alarm state. By pointing and clicking on the network element icon, systems management personnel execute element management applications using a web browser and perform more detailed management functions.

Inside the network, management of the physical and logical network elements is performed using a combination of the SNMP protocol and internal management application programming interfaces. Applications in the element manager use SNMP or other management APIs to perform network management functions.

Architecturally, the element management system includes of two distinct sets of functional elements. The first set of functional elements, including the configuration data server, performance data monitor and health/status monitor and network element recovery software, executes on an HA server equipped with RAID disks. The second set of functional elements, including the management applications, executes on a dedicated, non-HA management system. Even if the element manager system becomes non-operational, the network elements continue to be able to run and report alarms and even be able to recover from fault conditions. However, since all the management applications execute in the non-HA element manager, if the element manager goes down, then recovery actions requiring human intervention are not possible until the element manager becomes operational.

The wireless hubs (WHs) in the base stations are typically owned by a wireless service provider (WSP), and they are connected to the WSP's registration server (RS) either via point-to-point links, intranets or the Internet. The WSP's registration server is typically a software module executing on a processor to perform certain registration functions. Inter-working function units (IWF units) are typically software modules executing on a processor to perform certain interfacing functions. IWF units are typically connected to the registration servers via intranets/WAN, and the IWF units are typically owned by the WSP. However, the IWF units need not be located within the same LAN as the registration servers. Typically, accounting and directory servers (also software modules executing on a processor) are connected to the registration servers via a LAN in the service provider's Data Center (e.g., a center including one or more processors that hosts various servers and other software modules). Traffic from the end system is then routed via a router (connected to the LAN) to the public Internet or to an ISP's intranet. The registration server located in a foreign WSP's network is referred to as the foreign registration server (FRS), and the registration server located in the end system's home network (where the mobile purchases its service) is referred

to as the home registration server (HRS). The inter-working function unit in the home network is referred to as the home IWF while the inter-working function unit in the foreign network (i.e., the network the end system is visiting) is referred to as the serving IWF.

For fixed wireless service (i.e., a non-moving end system), an end system may register for service on the home network from the home network (e.g., at home service) or from a foreign network (e.g., roaming service). The end system receives an advertisement sent by an agent (e.g., an agent function implemented in software) in the wireless hub via the access point. There are both MAC-layer registration as well as network-layer registration to be accomplished.

For end systems at home (FIG. 23), the network layer registration (like a local registration) make's known to the home registration server the wireless hub to which the end system is currently attached. An IWF in the end system's home network will become the anchor or home IWF. Thus, PPP frames to and from the end system travel via the wireless hub to the home IWF in the home network. If the end system is at home, the home IWF is connected to the wireless hub via an XTunnel protocol.

For roaming wireless service (FIG. 24), the foreign registration server determines the identity of the home network of the roaming end system during the registration phase. Using this information, the foreign registration server communicates with the home registration server to authenticate and register the end system. The foreign registration server then assigns a serving IWF, and an I-XTunnel protocol connection is established between the home IWF and the serving IWF for the roaming end system. The serving IWF relays frames between the wireless hub and the home IWF. From the home IWF, data is sent to a PPP server (i.e., point-to-point protocol server) which may reside in the same IWF. However, if the data is to go to a corporate intranet or an ISP's intranet that has its own PPP server, the data is sent to the separate PPP server via the L2TP protocol. The separate server is typically owned and operated by an Internet service provider who is different from the wireless service provider. For the duration of the session, the locations of the home IWF and PPP server remain fixed. The MAC layer registration can be combined with the network registration to economize on the overhead of separate communications for MAC layer and network

layer registration; however, it may be advantageous to not combine these registration processes so that the WSP's equipment will be interoperable with other wireless networks that supports pure IETF Mobile-IP.

Registration sets up three tables. Table 1 is associated with each access point, and Table 1 identifies each connection (e.g., each end system) by a connection id (CID) and associates the connection id with a particular wireless (WM) modem address (i.e., the address of the end system or end system). Table 2 is associated with each wireless hub (WH), and Table 2 associates each connection id with a corresponding wireless modem address, access point and XTunnel id (XID). Table 3 is associated with each inter-working function (IWF), and Table 3 associates each connection id with a corresponding wireless modem address, wireless hub address, XTunnel id and IP port (IP/port). The entries described for these tables are described to include only relevant entries that support the discussion of mobility management. In reality, there are other important fields that need to be included as well.

Table 1: Connection Table at AP

CID	WM
C1	WM1
C2	WM1
C1	WM2

Table 2: Connection Table at WH

CID	WM	AP	XID
C1	WM1	AP1	5

C2	WM1	AP1	5
C1	WM2	AP1	6
C1	WM3	AP2	7

Table 3: Connection Table at IWF

CID	WM	WH	XID	IP/Port
C1	WM1	WH1	5	IP1/P1
C2	WM1	WH1	5	IP1/P2
C1	WM2	WH1	6	IP2/P3
C1	WM3	WH1	7	IP3/P1
C5	WM5	WH2	8	IP4/P1

The protocol stacks for dial-up users at home in a network as well as roaming users are illustrated in FIGS. 25-28. FIG. 25 depicts protocol stacks used for direct internet access by a fixed (i.e., non-moving) end system at home where a PPP protocol message terminates in the home IWF (typically collocated with the wireless hub) which relays message to and from an IP router and from there to the public internet. FIG. 26 depicts protocol stacks used for remote intranet access (i.e., either private corporate nets or an ISP) by a fixed (i.e., non-moving) end system at home where a PPP protocol message is relayed through the home IWF (typically collocated with the wireless hub) to a PPP server of the private corporate intranet or ISP. FIG. 27 depicts protocol stacks used for direct internet access by a roaming but fixed (i.e., non-moving) or a moving end system where the PPP protocol terminates in the home IWF (typically located in a mobile switching center of the home network) which relays message to and from an IP router. In FIG. 27, note how message traffic passes through a serving IWF (typically collocated with the wireless hub) in addition to the home IWF. FIG. 28 depicts protocol stacks used for remote intranet access (i.e., either private corporate nets or an ISP) by

a roaming but fixed (i.e., non-moving) or a moving end system where a PPP protocol message is relayed through the home IWF (typically located in a mobile switching center of the home network) to a PPP server of the private corporate intranet or ISP. In FIG. 28, note how message traffic passes through a serving IWF (typically collocated with the wireless hub) in addition to the home IWF. When the serving IWF and the wireless hub are co-located in the same nest of computers or are even programmed into the same computer, it is not necessary to establish a tunnel using the XTunnel protocol between the serving IWF and the wireless hub.

Equivalent variations to these protocol stacks (e.g. the RLP can be terminated at the wireless hub rather than at the serving IWF or home IWF for mobiles at home) are also envisioned. If the IWF is located far from the wireless hub, and the packets can potentially be carried over a lossy IP network between the IWF and wireless hub, then it would be preferred to terminate the RLP protocol at the wireless hub. Another variation is the Xtunnel between wireless hub and IWF need not be built on top of the UDP/IP. Xtunnels can be built using the Frame Relay/ATM link layer. However, the use of UDP/IP makes it easier to move the wireless hub and IWF software from one network to another.

Four types of handoff scenarios may occur, and they are labeled: (i) local mobility, (ii) micro mobility, (iii) macro mobility, and (iv) global mobility. In all four scenarios (in one embodiment of the invention), a route optimization option is not considered so that the locations of the home registration server and the ISP's PPP server do not change. In another embodiment of the invention with route optimization, the ISP's PPP server may change. However, this aspect is discussed below. In addition, the locations of the foreign registration server and IWF do not change in the first three scenarios.

The proposed IETF Mobile IP standard requires that whenever an end system changes the IP subnet to which it is attached, it sends a registration request message to a home agent in its home subnet. This message carries a care-of address where the end system can be reached in the new subnet. When traffic is sent, for example, from an ISP to an end system, the home agent intercepts the traffic that is bound for the end system as it that arrives in the home subnet, and then forwards the traffic to the care-of address.

The care-of address identifies a particular foreign agent in the foreign subnet. An end system's foreign agent can reside in the end system itself, or in a separate node that in turn forwards traffic to the end system (i.e., proxy registration agent). Mobile IP handoffs involve exchange of control messages between an end system's agent, the end system's home agent and potentially its corresponding hosts (CHs) (with route optimization option).

The proposed IETF Mobile IP standard would find it difficult meet the latency and scalability goals for all movements in a large internetwork. However, the present hierarchical mobility management meets such goals. For small movements (e.g. a change of Access Points), only MAC-layer re-registrations are needed. For larger movements, network-layer re-registrations are performed. The present hierarchical mobility management is different from the flat-structure used in the IETF proposed Mobile-IP standard as well as the serving/anchor inter-working function model used in cellular systems like CDPD (based on a standard sponsored by the Cellular Digital Packet Data forum).

As depicted in FIG. 29, the local mobility handoff handles end system (designated MN for mobile node) movement between APs that belong to the same wireless hub. Thus, only MAC layer re-registration is required. The end system receives a wireless hub advertisement from a new AP and responds with a registration request addressed to the new AP.

The new AP (i.e., the one that receives the registration request from the end system) creates new entries in its connection table and relays the registration message to its wireless hub. In local mobility handoffs, the wireless hub does not change. The wireless hub recognizes the end system's registration request as a MAC level registration request, and it updates its connection table to reflect the connection to the new AP. Then, the old AP deletes the connection entry from its connection table. There are at least three ways whereby the old AP can delete the old entries, namely (i) upon time out, (ii) upon receiving a copy of the relayed MAC layer association message from the new AP to the wireless hub (if this relay message is a broadcast message), and (iii) upon being informed by the wireless hub of the need to delete the entry.

As depicted in FIG. 30, the micro mobility handoff handles end system (designated MN for mobile node) movement between wireless hubs that belong to the same registration server and where the end system can still be served by the existing serving IWF. When an advertisement is received from a new wireless hub (through a new AP), the end system sends a message to request registration to the registration server. The registration request is relayed from the new AP to the new wireless hub to the registration server.

When the registration server determines that the existing IWF can still be used, the registration server sends a build XTunnel Request message to request the existing IWF to build an XTunnel to the new wireless hub. Later, the registration server sends a tear down XTunnel request message to request the existing IWF to tear down the existing XTunnel with the old wireless hub. The build and tear XTunnel Request messages can be combined into one message. A foreign registration server does not forward the registration message to the home registration server since there is no change of IWF, either the serving IWF or home IWF.

Upon receiving a positive build XTunnel reply and a positive tear XTunnel reply from IWF, the registration server sends a registration reply to end system. As the registration reply reaches the new wireless hub, the connection table at the new wireless hub is updated to reflect the connection to the new AP. The new AP updates its MAC filter address table and connection table after receiving a message from the new wireless hub, and the registration reply is forwarded to the end system.

The registration server sends a release message to the old wireless hub. When the old wireless hub receives the release message, it updates its connection table and the MAC filter address table and connection table of the old AP.

As depicted in FIG. 31, the macro mobility handoff case handles movement between wireless hubs that involves a change of the serving IWF in the foreign network, but it does not involve a change in the registration server. When an advertisement is received from a new wireless hub (through a new AP), the end system sends a message to request a network layer registration to the registration server. The registration request is relayed from the new AP to the new wireless hub to the registration server.

The registration server recognizes that it is a foreign registration server when the end system does not belong to the present registration server's network. This foreign registration server determines the identity of the home registration server by using a request, preferably a Radius Access request (RA request), to the foreign directory server (like a big yellow pages) and then assigns an appropriate IWF to be the serving IWF, and it forwards a registration request to the home registration server, preferably through a Radius Access request (RA request), informing the home registration server of the newly selected IWF.

The home registration server authenticates the registration request by using a request, preferably a Radius Access request (RA request), to the home directory server. Upon authenticating the request and determining that the existing home IWF can still be used, the home registration server instructs the home IWF to build a new I-XTunnel to the newly assigned serving IWF and to tear down the existing I-XTunnel to the old serving IWF. Upon receiving a positive build I-XTunnel reply and a positive tear I-XTunnel reply from the home IWF, the home registration server sends a registration reply to the foreign registration server.

The foreign registration server then instructs the newly assigned IWF to build an XTunnel to the new wireless hub. Upon receiving a positive build XTunnel reply, the foreign registration server instructs the old IWF to tear down the XTunnel to the old wireless hub. Upon receiving a positive build XTunnel reply and a positive tear XTunnel reply, the foreign registration server sends a registration reply to end system.

As the registration reply reaches the new wireless hub, the connection table at the new wireless hub is updated to reflect the connection to the new AP. The new AP updates its MAC filter address table and connection table after receiving a message from the new wireless hub, and the registration reply is forwarded to the end system.

The registration server sends a release message to the old wireless hub. When the old wireless hub receives the release message, it updates its connection table and the MAC filter address table, and the old AP updates its MAC filter address table and connection table after receiving a message from the old wireless hub.

The global mobility handoff case handles movement between wireless hubs that involves a change of registration servers. FIG. 32 depicts a global mobility handoff where the home IWF does not change, and FIG. 33 depicts a global mobility handoff where the home IWF changes. When an advertisement is received from a new wireless hub (through a new AP) in a new foreign network, the end system sends a message to request a network layer registration to the new foreign registration server. The registration request is relayed from the new AP to the new wireless hub to the new foreign registration server.

The registration server recognizes that it is a new foreign registration server when the end system does not belong to the present registration server's network. This foreign registration server determines the identity of the home registration server by using a request, preferably a Radius Access request (RA request), to the foreign directory server (like a big yellow pages) and then assigns an appropriate IWF to be the serving IWF, and it forwards the registration request to the home registration server, preferably through a Radius Access request (RA request), informing the home registration server of the newly selected IWF.

The home registration server authenticates the registration request by using a request, preferably a Radius Access request (RA request), to the home directory server. Upon authenticating the request and determining that the existing home IWF can still be used (FIG. 32), the home registration server instructs the home IWF to build a new I-XTunnel to the serving IWF newly assigned by the new foreign registration server. The home registration server also sends a de-registration message to the old foreign registration server and instructs the home IWF to tear down the existing I-XTunnel to the existing serving IWF of the old foreign network. Upon receiving a positive build I-XTunnel reply and a positive tear I-XTunnel reply from the home IWF, the home registration server sends a registration reply to the new foreign registration server.

The new foreign registration server then instructs the newly assigned IWF to build an XTunnel to the new wireless hub. Upon receiving a positive build XTunnel reply, the foreign registration server sends a registration reply to end system. As the registration reply reaches the new wireless hub, the connection table at the new wireless hub is updated to reflect the connection to the new AP. The new AP updates its MAC

filter address table and connection table after receiving a message from the new wireless hub, and the registration reply is forwarded to the end system.

The old foreign registration server instructs the old IWF to tear down the XTunnel to the old wireless hub. Upon receiving a positive tear XTunnel reply or contemporaneously with the tear down XTunnel request, the old foreign registration server sends a release message to the old wireless hub. When the old wireless hub receives the release message, it updates its connection table and the MAC filter address table, and the old AP updates its MAC filter address table and connection table after receiving a message from the old wireless hub.

Alternatively, after the home registration server authenticates the registration request from the new foreign registration server and determines that the existing home IWF cannot be used (FIG. 33), the home registration server chooses a new home IWF and instructs the new home IWF to build a new level 2 tunnel protocol tunnel (L2TP tunnel) to the present PPP server (e.g., the PPP server in a connected ISP intranet). Then, the home registration server instructs the old home IWF to transfer its L2TP tunnel traffic to the new home IWF.

Then the home registration server instructs the new home IWF to build a new I-XTunnel to the serving IWF newly assigned by the new foreign registration server. The home registration server also sends a de-registration message to the old foreign registration server and instructs the home IWF to tear down the existing I-XTunnel to the existing serving IWF of the old foreign network. Upon receiving a positive build I-XTunnel reply and a positive tear I-XTunnel reply from the home IWF, the home registration server sends a registration reply to the new foreign registration server.

The new foreign registration server then instructs the newly assigned IWF to build an XTunnel to the new wireless hub. Upon receiving a positive build XTunnel reply, the foreign registration server sends a registration reply to end system. As the registration reply reaches the new wireless hub, the connection table at the new wireless hub is updated to reflect the connection to the new AP. The new AP updates its MAC filter address table and connection table after receiving a message from the new wireless hub, and the registration reply is forwarded to the end system.

The old foreign registration server instructs the old IWF to tear down the XTunnel to the old wireless hub. Upon receiving a positive tear XTunnel reply or contemporaneously with the tear down XTunnel request, the old foreign registration server sends a release message to the old wireless hub. When the old wireless hub receives the release message, it updates its connection table and the MAC filter address table, and the old AP updates its MAC filter address table and connection table after receiving a message from the old wireless hub.

End systems constructed according to the present invention interoperate with networks constructed according to the proposed IETF Mobile-IP standards, and end systems constructed according to the proposed IETF Mobile-IP standards interoperate with networks constructed according to the present invention.

The main differences between the present invention and the IETF Mobile-IP (rfc2002, a standards document) are:

(i) The present invention uses a hierarchical concept for mobility management rather than a flat structure as in the proposed IETF Mobile-IP standard. Small mobility within a small area does not result in a network level registration. Micro mobility involves setting up of a new Xtunnel and tearing down of an existing Xtunnel. Global mobility, at the minimum, involves setting up of a new I-XTunnel and tearing down of an existing I-Xtunnel apart from the setting up/tearing down of XTunnel. Global mobility sometimes also involves setting up a new L2TP Tunnel and transferring of L2TP state from the existing L2TP Tunnel to the new L2TP Tunnel.

(ii) In the present invention, a user name plus a realm is used to identify a remote dial-up user rather than a fixed home address as in the case of the proposed IETF Mobile-IP standard.

(iii) In the present invention, registration and routing functions are carried out by separate entities. The two functions are carried out by the home agent in the proposed IETF Mobile IP standard, and both functions are carried

out by the foreign agent in the proposed IEFT Mobile IP standard. In contrast, in an embodiment of the present invention, registration is carried out in the registration server and routing functions are carried out by both the home and foreign IWF and the wireless hub (also referred to as the access hub).

(iv) The present invention utilizes three tunnels per PPP session. The XTunnel is more of a link-layer tunnel between the wireless hub and the serving IWF. The I-XTunnel between the serving IWF and the home IWF is more like the tunnel between home and foreign agents in the proposed IETF Mobile-IP standard. The L2TP tunnel is used only when home IWF is not a PPP server.

(v) In the present invention, network layer registration occurs before PPP session starts while in the proposed IETF Mobile-IP standard, Mobile-IP registration occurs after PPP session enters into the open state.

(vi) In the present invention, the network entity that advertises the agent advertisement (i.e., the wireless hub) is not on a direct link to the end systems whereas for the proposed IETF Mobile-IP standard, the agent advertisement must have a TTL of 1 which means that the end systems have a direct link with the foreign agent. In addition, the agent advertisement in the present invention is not an extension to the ICMP router advertisements as in the proposed IETF Mobile-IP standard.

End systems in the present invention, should support agent solicitation. When an end system in the present invention visits a network which is supporting the proposed IETF Mobile-IP standard, it waits until it hears an agent advertisement. If it does not receive an agent advertisement within a reasonable time frame, it broadcasts an agent solicitation.

In the present invention, network operators may negotiate with other networks that support the proposed IETF Mobile-IP standard such that home addresses can be assigned to the end systems of the present invention that wish to use other networks.

When the end system of the present invention receives the agent advertisement, it can determine that the network it is visiting is not an a network according to the present invention and hence uses the assigned home address to register.

For networks supporting the proposed IETF Mobile-IP standard, the PPP session starts before Mobile-IP registration, and the PPP server is assumed to be collocated with the foreign agent in such networks. In one embodiment, an SNAP header is used to encapsulate PPP frames in the MAC frames of the present invention (in a manner similar to Ethernet format), and the foreign agent interprets this format as a proprietary PPP format over Ethernet encapsulation. Thus, the end system of the present invention and its PPP peer can enter into an open state before the foreign agent starts transmitting an agent advertisement, and the end system of the present invention can register.

To allow end systems supporting the proposed IETF Mobile-IP standard to work in networks of the type of the present invention, such mobiles are at least capable of performing similar MAC layer registrations. By making the agent advertisement message format similar to the proposed Mobile-IP standard agent advertisement message format, a visiting end system can interpret the agent advertisement and register with a wireless hub. In the present invention, registration request and reply messages are similar to the proposed IETF Mobile-IP standard registration request and reply messages (without any unnecessary extensions) so that the rest of the mobility management features of the present invention are transparent to the visiting end systems.

Since end systems supporting the proposed IETF Mobile-IP standard expect a PPP session to start before Mobile-IP registration, an optional feature in wireless hubs of the present invention starts to interpret PPP LCP, NCP packets after MAC-layer registrations.

To avoid losing traffic during handoffs, the mobility management of the present invention uses the make before break concept. For local mobility, a make before break connection is achieved by turning the MAC-layer registration message relayed by the new AP to the wireless hub into a broadcast message. That way, the old AP can hear

about the new registration and forward packets destined for the end system that have not been transmitted to the new AP.

For micro mobility, information about the new wireless hub is included in the Tear XTunnel message exchanged between the serving IWF and the old WH. That way, the old wireless hub can forward buffered packets to the new wireless hub upon hearing a TearXTunnel message from the serving IWF. Alternatively, the RLP layer at the IWF knows the sequence number that has been acknowledged by the old wireless hub so far.

At the same time, the IWF knows the current send sequence number of the latest packet sent to the old wireless hub. Therefore, the IWF can forward those packets that are ordered in between these two numbers to the new wireless hub before sending newer packets to the new wireless hub. The RLP layer is assumed to be able to filter duplicate packet. The second approach is probably preferable to the first approach for the old wireless hub may not be able to communicate with one another directly.

For macro mobility, the old serving IWF can forward packets to the new serving IWF, in addition to the packet forwarding done from the old wireless hub to the new wireless. All we need to do is to forward the new serving IWF identity to the new serving IWF in the tear down I-XTunnel message. Another way to achieve the same result is to let the home IWF forward the missing packets to the new serving IWF rather than asking the old serving IWF to do the job since the home IWF knows the I-XTunnel sequence number last acknowledged by the old serving IWF and the current I-XTunnel sequence number sent by the home IWF.

The method of estimating how much buffer should be allocated per mobile per AP per wireless hub per IWF such that the traffic loss between handoffs can be minimized is to let the end system for the AP for the wireless hub for the IWF estimate the packet arrival rate and the handoff time. This information is passed to the old AP of the wireless hub of the IWF to determine how much traffic should be transferred to the new AP of the wireless hub of the IWF, respectively, upon handoffs.

To achieve route optimization in the present invention, the end system chooses the PPP server closest to the serving IWF. Without route optimization, excessive transport delays and physical line usage may be experienced.

For example, an end system subscribed to a home network in New York City may roam to Hong Kong. To establish a link to a Hong Kong ISP, the end system would have a serving IWF established in a wireless hub in Hong Kong and a home IWF established in the home network in New York City. A message would then be routed from the end system (roamed to Hong Kong) through the serving IWF (in Hong Kong) and through the home IWF (in New York City) and back to the Hong Kong ISP.

A preferred approach is to connect from the serving IWF (in Hong Kong) directly to the Hong Kong ISP. The serving IWF acts like the home IWF. In this embodiment, roaming agreements exist between the home and foreign wireless providers. In addition, the various accounting/billing systems communicate with one another automatically such that billing information is shared. Accounting and billing information exchange may be implemented using standards such as the standard proposed by the ROAMOPS working group of the IETF.

However, the serving IWF must still discover the closest PPP server (e.g., the Hong Kong ISP). In the present embodiment, the foreign registration server learns of the end system's desire to connect to a PPP server (e.g., a Hong Kong ISP) when it receives a registration request from the end system. When the foreign registration server determines that the serving IWF is closer to the desired PPP server (e.g., the Hong Kong ISP) than the home IWF is, the foreign registration server instructs the serving IWF to establish an L2TP tunnel to its nearest PPP server (in contrast to the PPP server closest to the home registration server and home IWF). Then, the foreign registration server informs the home registration server that the end system is being served by the serving IWF and the foreign PPP.

In an alternative embodiment, the foreign registration server determines that the serving IWF is closer to the desired PPP server (e.g., the Hong Kong ISP) than the home IWF is, when it receives a registration request from the end system. The foreign registration server relays the registration request message to the home registration server

with an attached message indicating the serving IWF information and a notification that route optimization is preferred. At the same time, the foreign registration server instructs the serving IWF to establish an L2TP tunnel to the PPP server. Upon approving the registration request, the home registration server instructs the home IWF to transfer the L2TP state to the foreign IWF.

In FIG. 34, data frames are initially communicated between the first mobile end system and the first access hub through the first access point. Then, a registration request is sent from the first mobile end system through the second access point to the first access hub to re-register the first mobile end system with the first access hub without informing the first registration server when the first mobile end system moves and re-registers through the second access point. Finally, the second access point is linked with the first access hub when the first mobile end system re-registers through the second access point, and the first access point is de-linked from the first access hub when the second access point is linked with the first access hub.

In FIG. 35, data frames are initially communicated between the first mobile end system and the first inter-working function through the first access hub. Then, a registration request is sent from the first mobile end system through a first access point and through the second access hub to the first registration server to re-register the first mobile end system with the first registration server without informing the home registration server when the first mobile end system moves and re-registers through the second access hub. Finally, the second access hub is linked with the first inter-working function when the first mobile end system re-registers through the second access hub, and the first access hub is de-linked from the first inter-working function after the second access hub is linked with the first inter-working function.

In FIG. 36, data frames are initially communicated between the first mobile end system and the third inter-working function through the first inter working function, and data frames are initially communicated between the third inter-working function and the first communications server. Then, a registration request is sent from the first mobile end system through a first access point and through the first access hub and through the first registration server to the home registration server to re-register the first mobile end system with the home registration server without de-linking the third inter-working

function from the first communications server when the first mobile end system moves and re-registers through the first access hub. The step of sending the registration request from the first registration server to the home registration server sends an indication of a change from the first inter-working function to the second inter-working function. Finally, the second inter-working function is linked with the third inter-working function when the first mobile end system re-registers through the first access hub, and the first inter-working function is de-linked from the third inter-working function after the second inter-working function is linked with the third inter-working function.

In FIG. 37, data frames are initially communicated between a first mobile end system and the third inter-working function through the first inter-working function, and data frames are initially communicated between the third inter-working function and the first communications server. Then, a registration request is sent from the first mobile end system through a first access point and through the first access hub and through the second registration server to the home registration server to re-register the first mobile end system with the home registration server without de-linking the third inter-working function from the first communications server when the first mobile end system moves and re-registers through the first access hub. Finally, the third inter-working function is linked with the second inter-working function when the first mobile end system re-registers through the first access hub, and the third inter-working function is de-linked from the first inter-working function after the third inter-working function is linked with the second inter-working function.

In FIG. 38, data frames are initially communicated between a first mobile end system and the third inter-working function through the first inter-working function, and data frames are initially communicated between the third inter-working function and the first communications server. Then, a registration request is sent from the first mobile end system through a first access point and through the first access hub and through the second registration server to the home registration server to re-register the first mobile end system with the home registration server when the first mobile end system moves and re-registers through the first access hub. Finally, the fourth inter-working function is linked with the second inter-working function when the first mobile end system re-registers through the first access hub, the fourth inter-working function is linked with the

first communications server, the third inter-working function is de-linked from the first communications server when the fourth inter-working function is linked with the first communications server, and the third inter-working function is de-linked from the first inter-working function after the fourth inter-working function is linked with the second inter-working function.

The wireless data network include a home mobility switching center, a foreign mobility switching center, a base station and an end user. The home mobility switching center includes a home registration server and a home inter-working function. The foreign mobility switching center includes a serving registration server and a serving inter-working function. The base station includes a proxy registration agent. The end user modem includes a user registration agent. The user registration agent is coupled to the proxy registration agent, the proxy registration agent is coupled to the serving registration server, and the serving registration server is coupled to the home registration server. The proxy registration agent includes a module to send an advertisement containing a care-of-address when the proxy registration agent receives a solicitation from the user registration agent, and the user registration agent includes a module to incorporate user identity information and the care-of-address in a registration request when the user registration agent receives the advertizement and a module to send this registration request to the proxy registration agent. The proxy registration agent includes a module to forward to the serving registration server any registration request received from any user. The serving registration server includes a foreign directory module to determine a home registration server address, a module to encapsulate the registration request and incorporate serving registration server identity information and the encapsulated registration request in a radius access request when the home registration server address is determined, and a module to send the radius access request to the home registration server. The home registration server includes a home directory module to authenticate the serving registration server identity information, a module to form an inter-working function request from the radius access request when the serving registration server identity information is authenticated, and a module to send the inter-working request to the home inter-working function.

Having described preferred embodiments of a novel network architecture with wireless end users able to roam (which are intended to be illustrative and not limiting), it is noted that modifications and variations can be made by persons skilled in the art in light of the above teachings. For example, connection links described herein may make reference to known connection protocols (e.g., IP, TCP/IP, L2TP, IEEE 802.3, etc.); however, the invention contemplates other connection protocols in the connections links that provide the same or similar data delivery capabilities. Acting agents in the above described embodiments may be in the form of software controlled processors or may be other form of controls (e.g., programmable logic arrays, etc.). Acting agents may be grouped as described above or grouped otherwise in keeping with the connection teachings described herein and subject to security and authentication teachings as described herein. Furthermore, a single access point, access hub (i.e., wireless hub) or inter-working function unit (IWF unit) may provide multi-channel capability. Thus, a single access point or access hub or IWF unit may act on traffic from multiple end systems, and what is described herein as separate access points, access hubs or IWF units contemplates equivalence with a single multi-channel access point, access hub or IWF unit. It is therefore to be understood that changes may be made in the particular embodiments of the invention disclosed which are within the scope and spirit of the invention as defined by the appended claims.

Having thus described the invention with the details and particularity required by the patent laws, what is claimed and desired protected by Letters Patent is set forth in the appended claims.

4. Brief Description Of Drawings

The invention will be described in detail in the following description of preferred embodiments with reference to the following figures wherein:

FIG. 1 is a configuration diagram of a known remote access architecture through a public switched telephone network;

FIG. 2 is a configuration diagram of a remote access architecture through a wireless packet switched data network according to the present invention;

FIG. 3 is a configuration diagram of selected parts of the architecture of the network of FIG. 2 showing a roaming scenario;

FIG. 4 is a configuration diagram of a base station with local access points;

FIG. 5 is a configuration diagram of a base station with remote access points;

FIG. 6 is a configuration diagram of a base station with remote access points, some of which are connected using a wireless trunk connection;

FIG. 7 is a diagram of a protocol stack for a local access point;

FIG. 8 is a diagram of a protocol stack for a remote access point with a wireless trunk;

FIG. 9 is a diagram of a protocol stack for a relay function in the base station for supporting remote access points with wireless trunks;

FIG. 10 is a diagram of protocol stacks for implementing the relay function depicted in FIG. 9;

FIG. 11 is a diagram of protocol stacks for a relay function in the base station for supporting local access points;

FIG. 12 is a configuration diagram of selected parts of the architecture of the network of FIG. 2 showing a first end system registering in the home network from the home network and a second system registering in the home network from a foreign network using a home inter-working function for an anchor;

FIG. 13 is a configuration diagram of selected parts of the architecture of the network of FIG. 2 showing a first end system registering in the home network from the home network and a second system registering in the home network from a foreign network using a serving inter-working function for an anchor;

FIG. 14 is a ladder diagram of the request and response messages to register in a home network from a foreign network and to establish, authenticate and configure a data link;

FIG. 15 is a configuration diagram of selected parts of the architecture of the network of FIG. 2 showing registration requests and responses for registering a mobile in a home network from the home network;

FIG. 16 is a configuration diagram of selected parts of the architecture of the network of FIG. 2 showing registration requests and responses for registering a mobile in a home network from a foreign network;

FIG. 17 is a configuration diagram of protocol stacks showing communications between an end system in a home network and an inter-working function in the home network where the cell site has local access points;

FIG. 18 is a configuration diagram of protocol stacks showing communications between an end system in a home network and an inter-working function in the home network where the cell site has remote access points coupled to a wireless hub through a wireless trunk;

FIG. 19 is a configuration diagram of protocol stacks showing communications between a base station coupled to a roaming end system and a home inter-working function;

FIG. 20 is a configuration diagram of protocol stacks showing communications between an end system in a home network through an inter-working function in the home network to an internet service provider;

FIG. 21 is a configuration diagram of protocol stacks showing communications between an end system in a foreign network and a home registration server in a home network during the registration phase;

FIG. 22 is a processing flow diagram showing the processing of accounting data through to the customer billing system;

FIGS. 23 and 24 are ladder diagrams depicting the registration process for an end system in a home network and in a foreign network, respectively;

FIGS. 25 and 26 are protocol stack diagrams depicting an end system connection in a home network where a PPP protocol terminates in an inter-working function of the home network and where the PPP protocol terminates in an ISP or intranet, respectively;

FIGS. 27 and 28 are protocol stack diagrams depicting an end system connection in a foreign network where a PPP protocol terminates in an inter-working function of the foreign network and where the PPP protocol terminates in an ISP or intranet, respectively;

FIGS. 29, 30 and 31 are ladder diagrams depicting a local handoff scenario, a micro handoff scenario and a macro handoff scenario, respectively;

FIG. 32 is a ladder diagram depicting a global handoff scenario where the foreign registration server changes and where home inter-working function does not change;

FIG. 33 is a ladder diagram depicting a global handoff scenario where both the foreign registration server and the home inter-working function change;

FIGS. 34, 35 and 36 are functional flow charts depicting local, micro and macro handoff procedures according to the present invention;

FIG. 37 is a functional flow chart depicting global handoff procedures according to the present invention when the inter-working function in the home network does not change; and

FIG. 38 is a functional flow chart depicting global handoff procedures according to the present invention when the inter-working function in the home network does change.

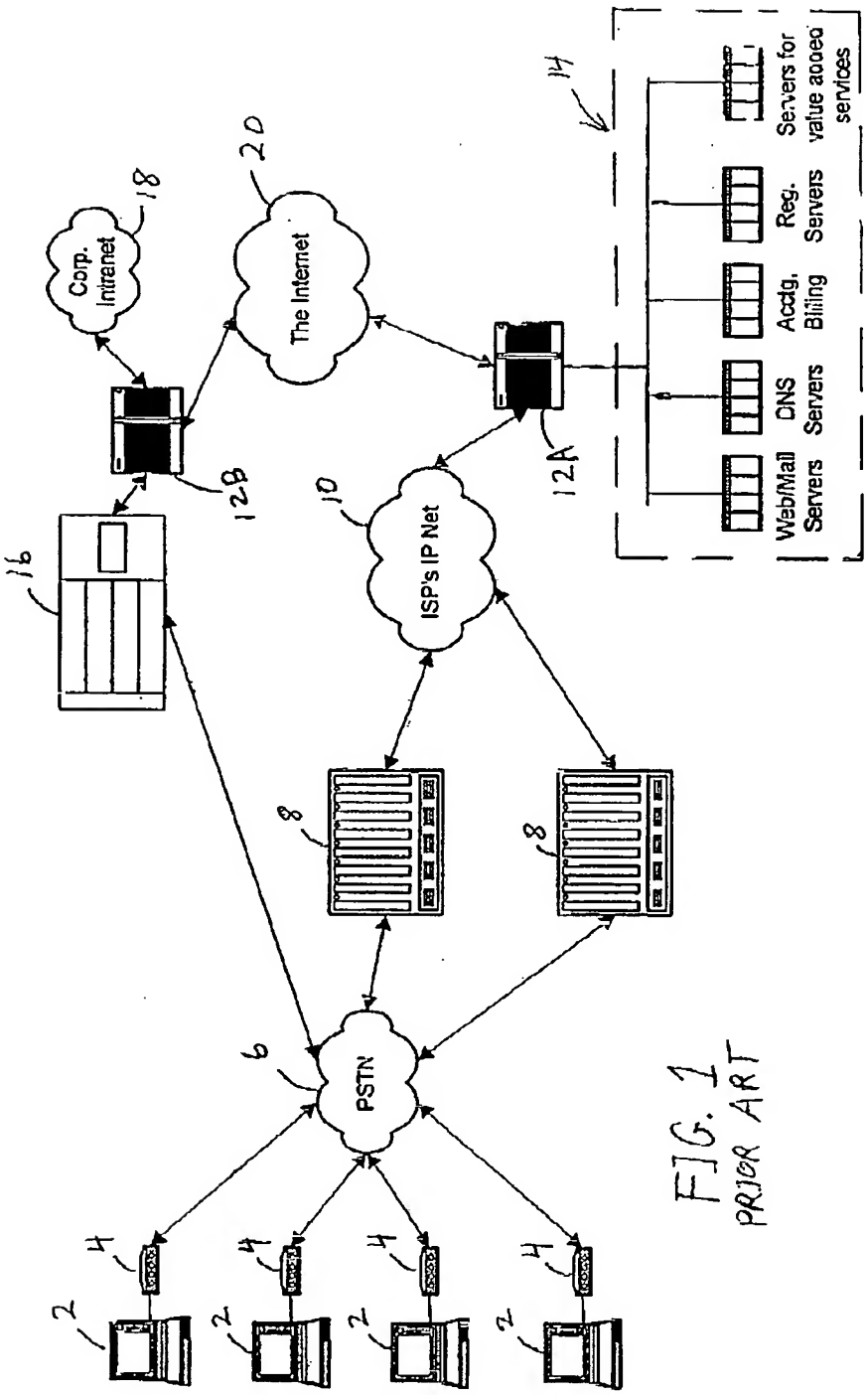


FIG. 1
PRIOR ART

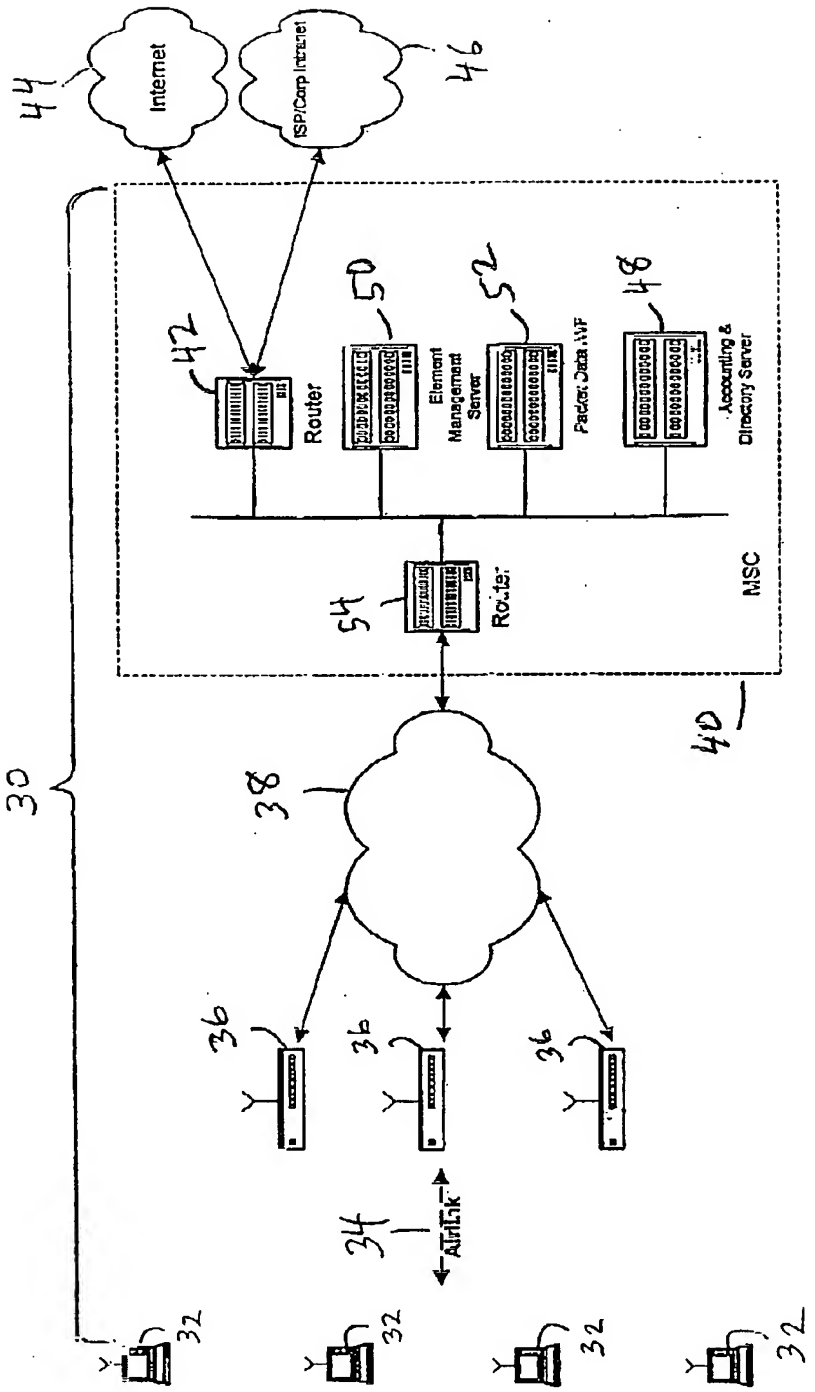

Internet
ISP/Corp Intranet
44
46
42
Router
50
Element Management Server
52
Packet Data IWF
48
Accounting & Directory Server
MSC
54
Router
40
38
30
36
36
36
34
AirLink
32
32
32
32

FIG. 2

FIG. 3

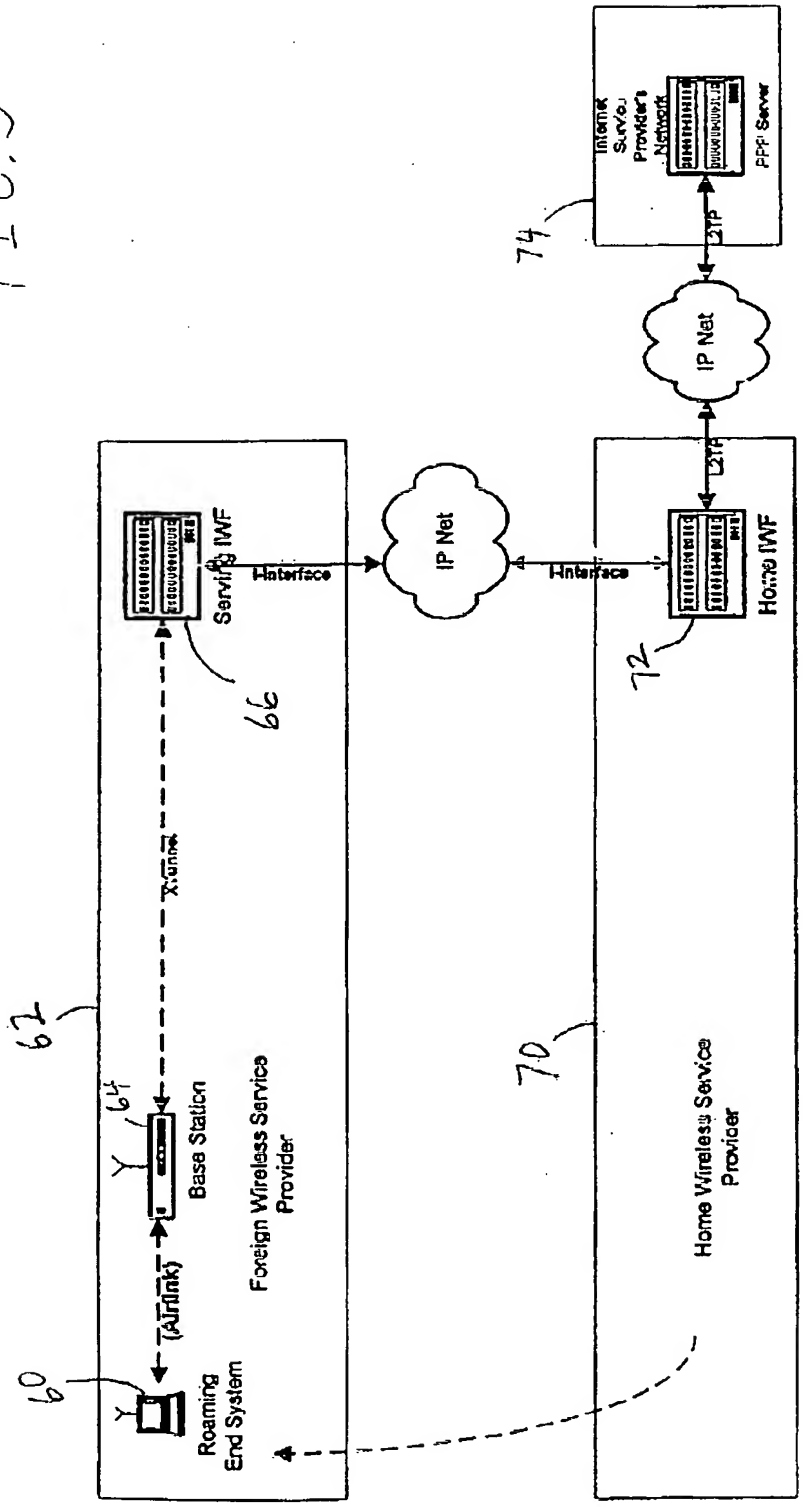

Internet Service Provider's Network
PPP Server
74
L2TP
IP Net
L2TP
Home IWF
72
Interface
IP Net
Interface
Serving IWF
66
Home Wireless Service Provider
70
Foreign Wireless Service Provider
62
Base Station
64
(Airlink)
Roaming End System
60

FIG. 4

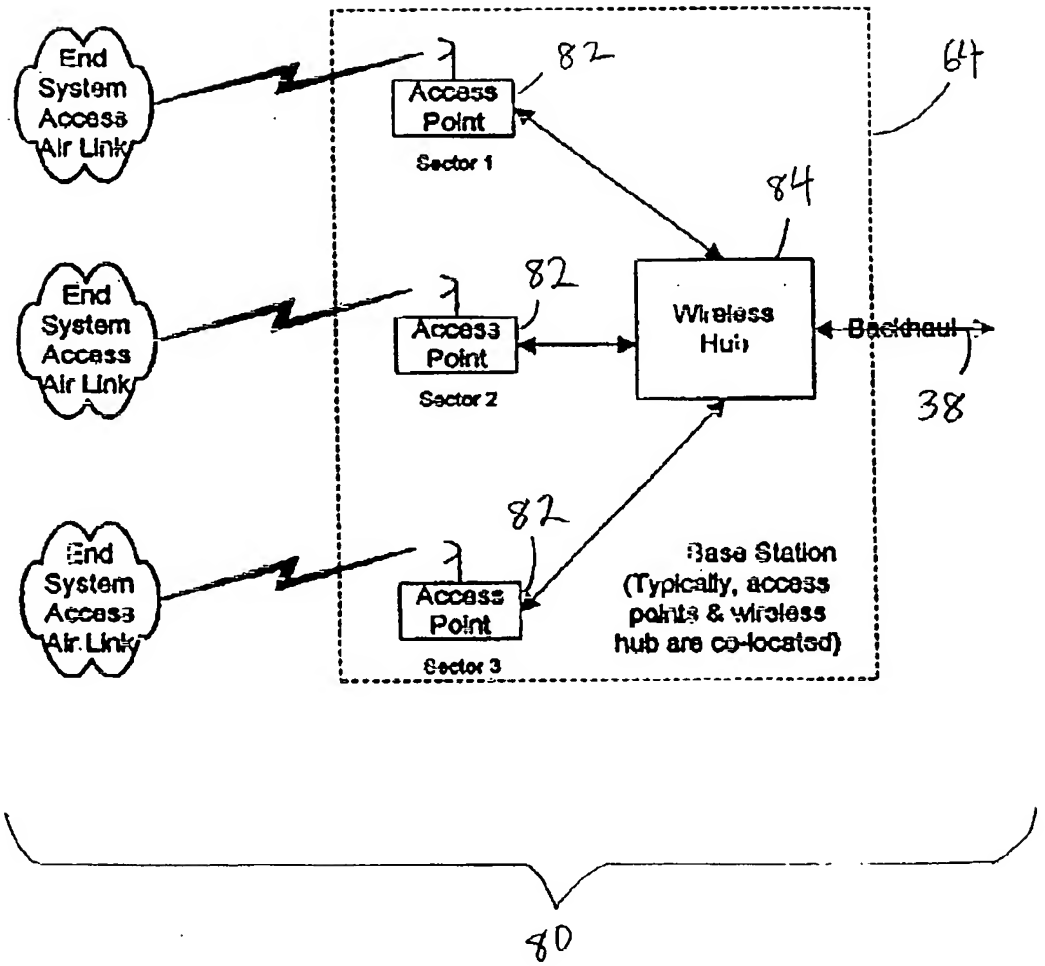

End System Access Air Link
End System Access Air Link
End System Access Air Link
Access Point
Sector 1
Access Point
Sector 2
Access Point
Sector 3
82
82
82
84
Wireless Hub
Backhaul
38
64
Base Station
(Typically, access points & wireless hub are co-located)
80

FIG. 5

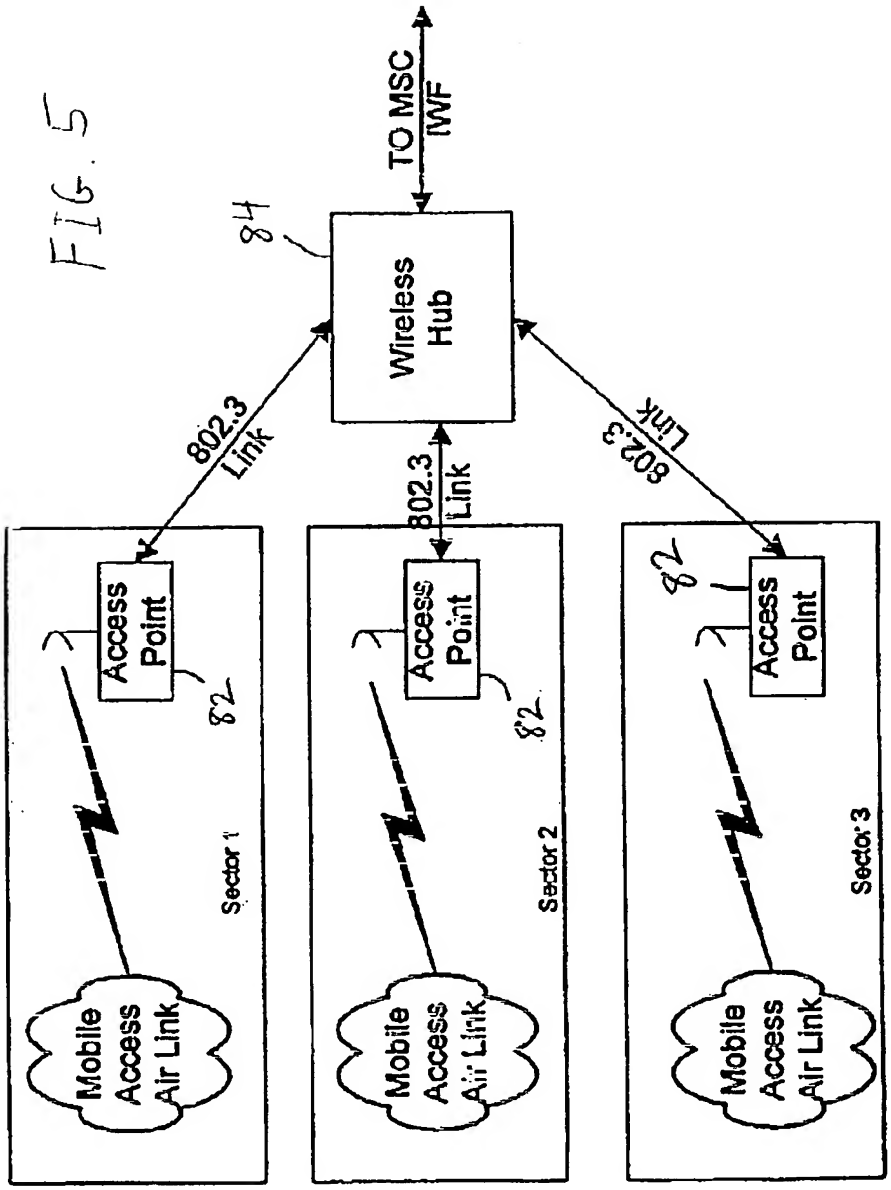
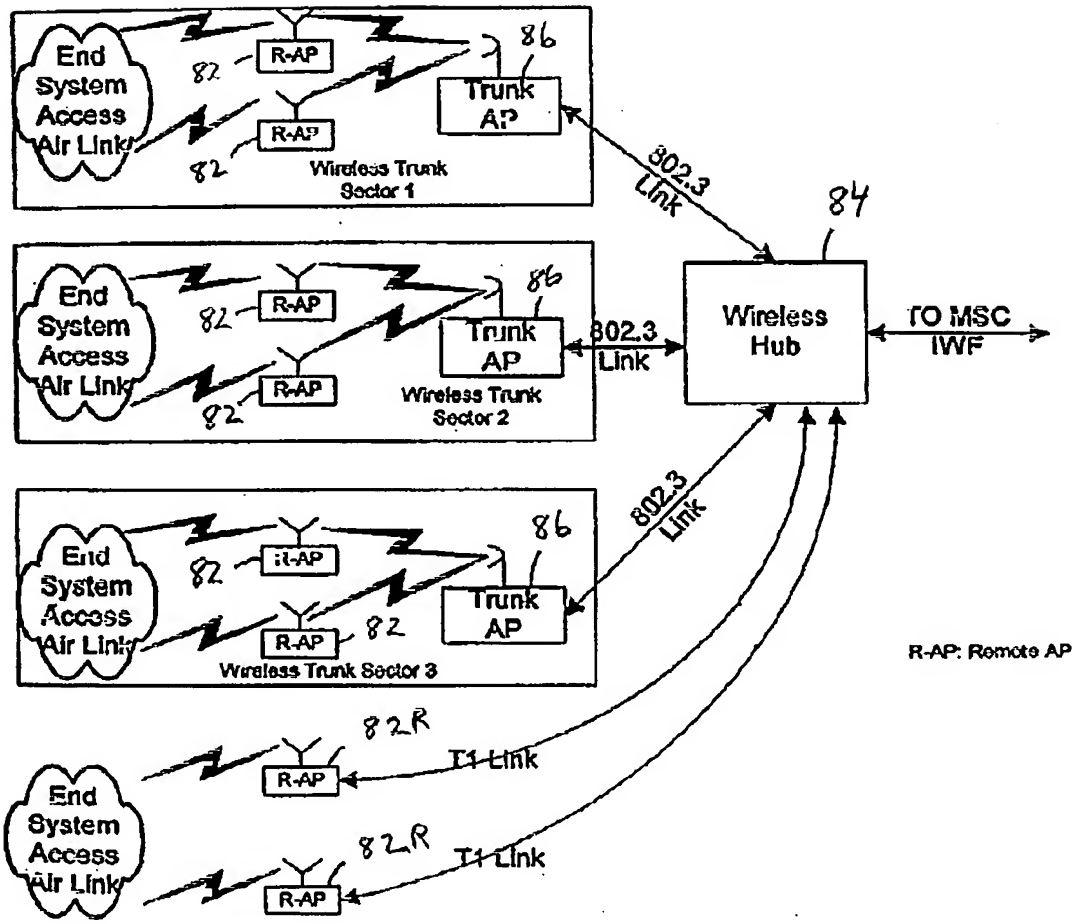

TO MSC
IWF
84
Wireless Hub
802.3 Link
802.3 Link
802.3 Link
82
82
82
Access Point
Access Point
Access Point
Mobile Access Air Link
Mobile Access Air Link
Mobile Access Air Link
Sector 1
Sector 2
Sector 3

FIG. 6


End System Access Air Link
R-AP
82
86
Trunk AP
Wireless Trunk Sector 1
802.3 Link
84
Wireless Hub
TO MSC IWF
Wireless Trunk Sector 2
Wireless Trunk Sector 3
R-AP: Remote AP
82R
T1 Link

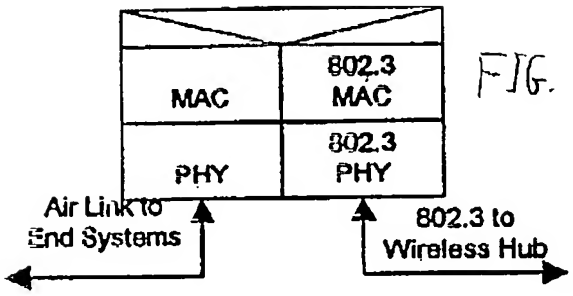


FIG. 7

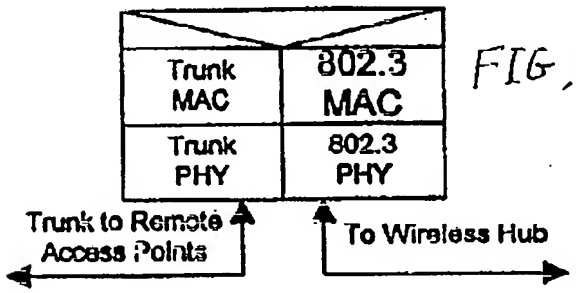


FIG. 8

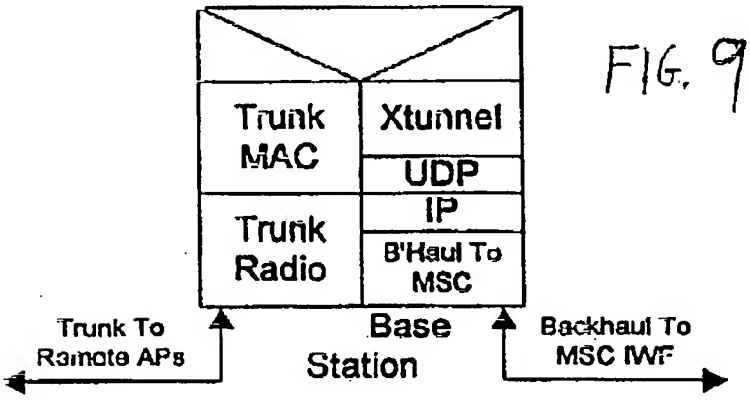


FIG. 9

FIG. 10

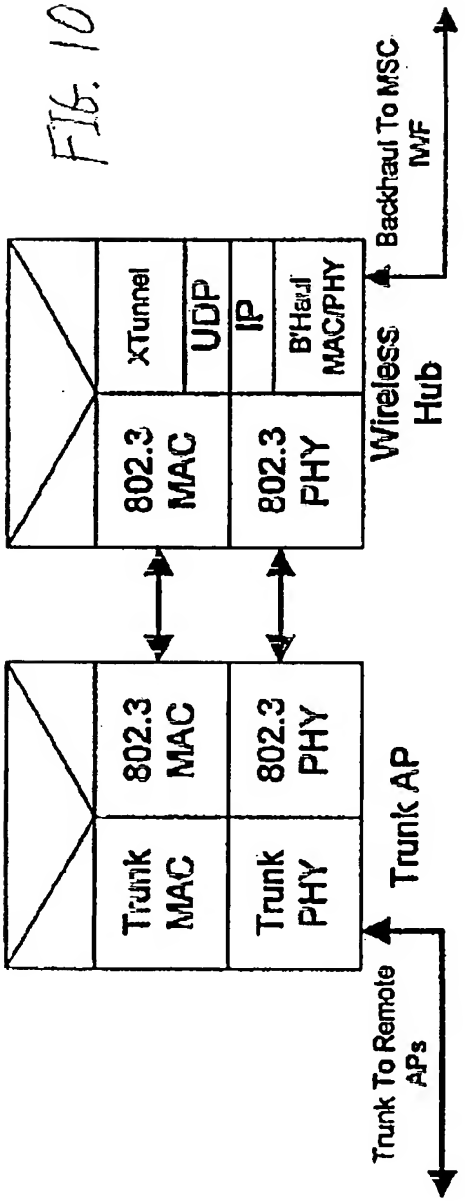
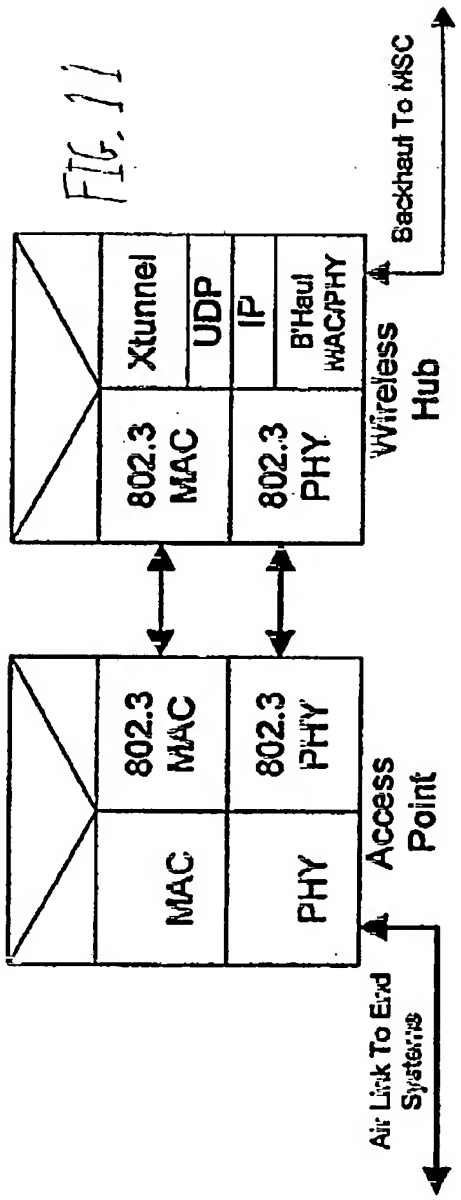

Backhaul To MSC IWF
Wireless Hub
xTunnel
UDP
IP
B'Haul MAC/PHY
802.3 MAC
802.3 PHY
Trunk MAC
Trunk PHY
Trunk AP
Trunk To Remote APs

FIG. 11


Backhaul To MSC
Wireless Hub
Xtunnel
UDP
IP
B'Haul MAC/PHY
802.3 MAC
802.3 PHY
Access Point
MAC
PHY
Air Link To End Systems

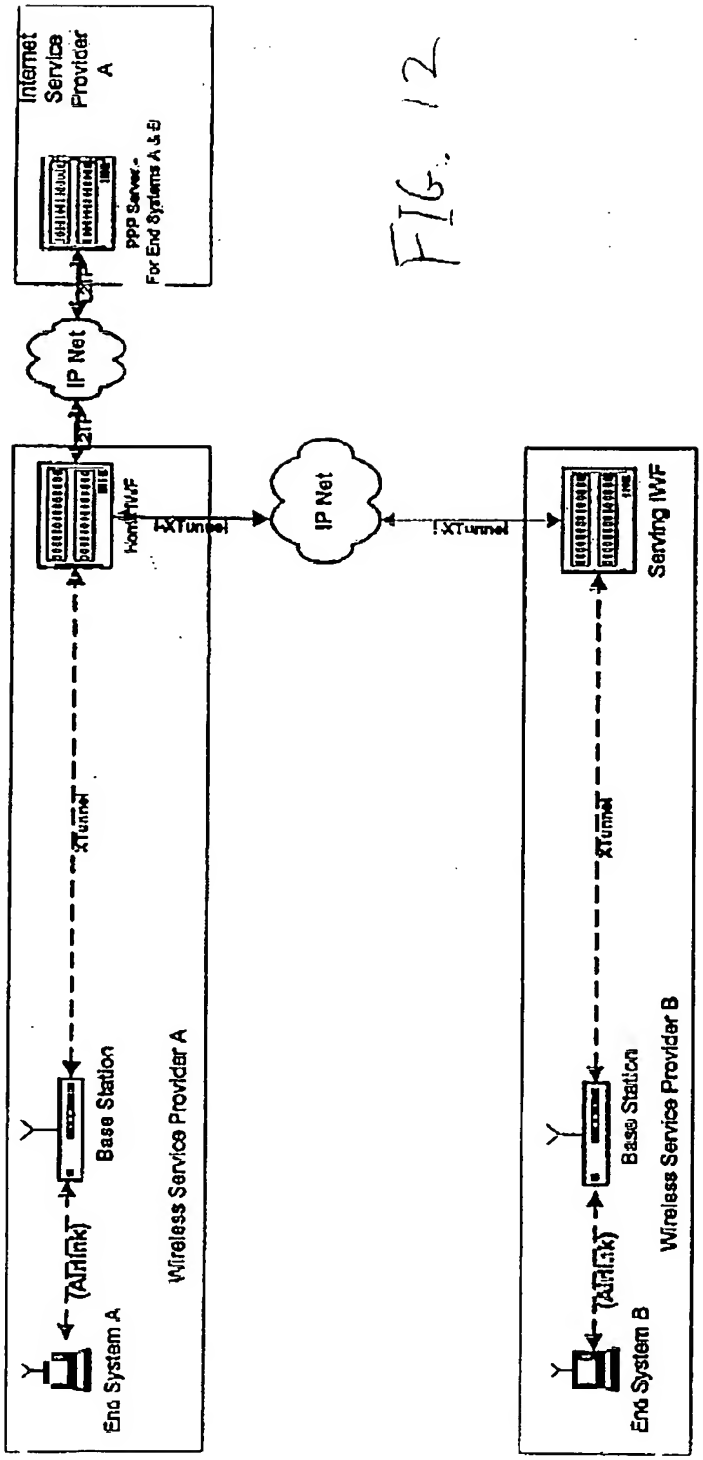

Internet Service Provider A
PPP Server - For End Systems A & B
IP Net
IP
Home IWF
IXTunnel
IP Net
IXTunnel
Serving IWF
XTunnel
XTunnel
Base Station
Base Station
(AirLink)
(AirLink)
End System A
End System B
Wireless Service Provider A
Wireless Service Provider B

FIG. 12

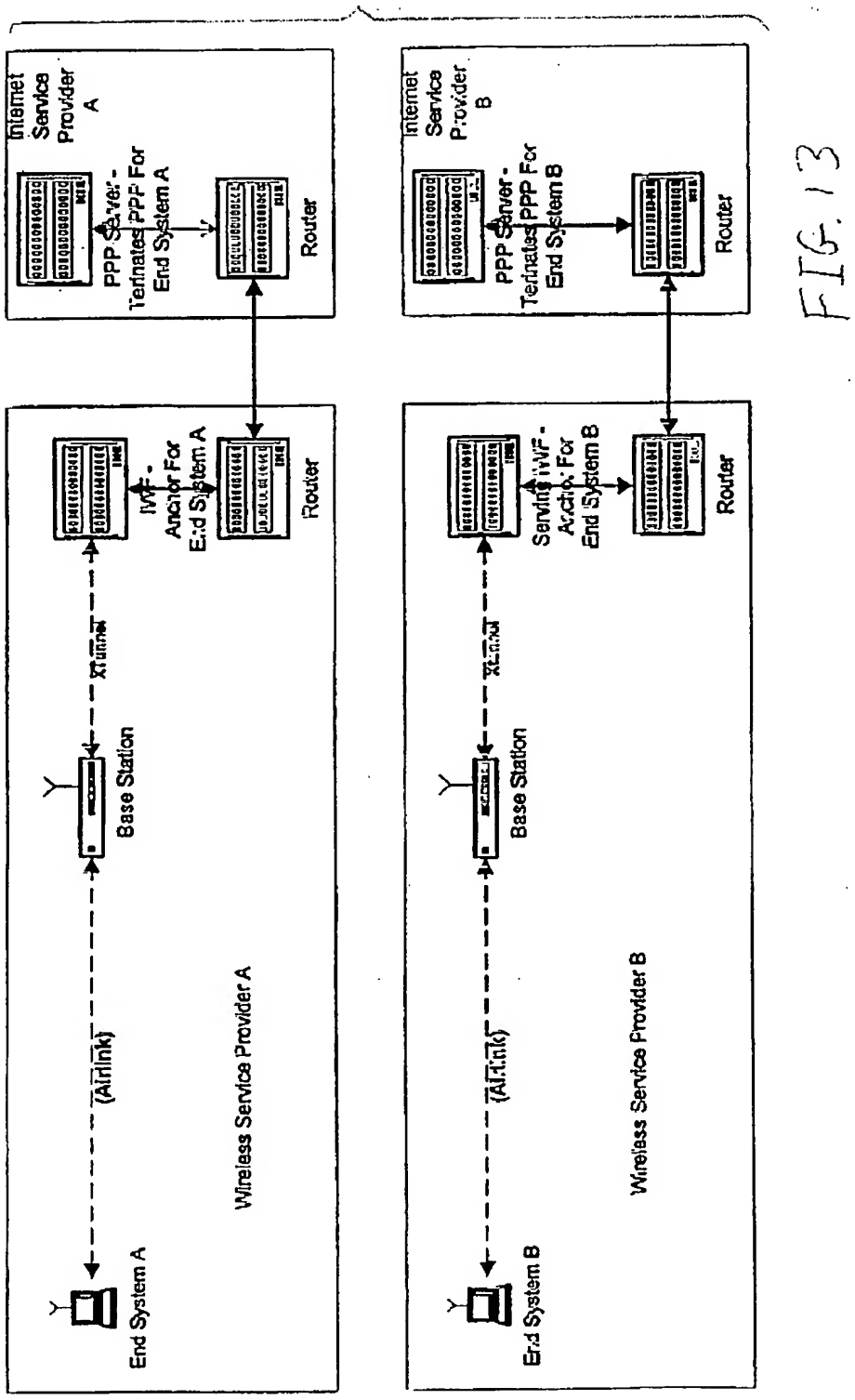

Internet Service Provider A
PPP Server - Terminates PPP For End System A
Router
IWF - Anchor For End System A
Router
Base Station
(Airlink)
End System A
Wireless Service Provider A
Internet Service Provider B
PPP Server - Terminates PPP For End System B
Router
Serving IWF - Anchor For End System B
Router
Base Station
(Airlink)
End System B
Wireless Service Provider B

FIG. 13

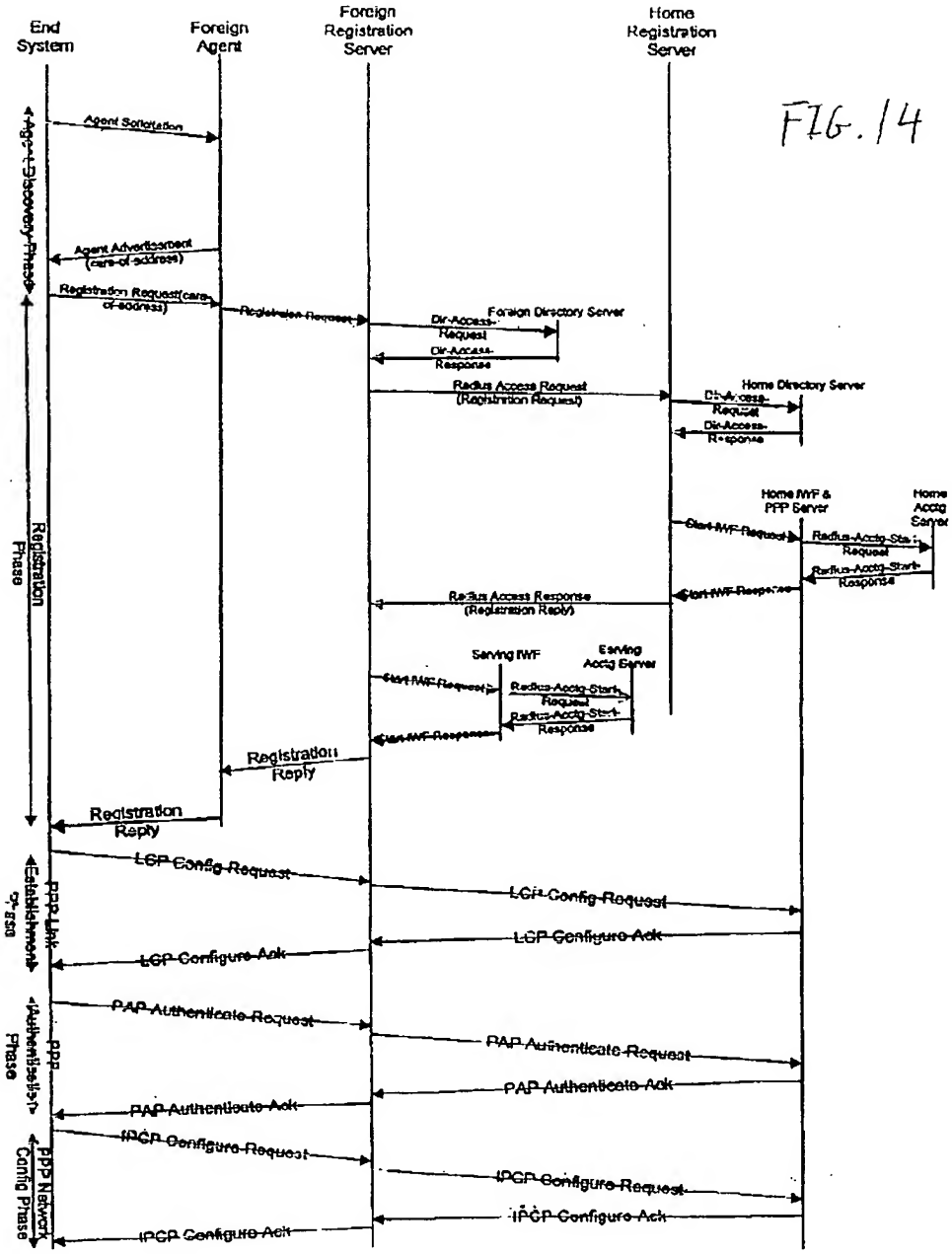

End System
Foreign Agent
Foreign Registration Server
Home Registration Server
Agent Solicitation
Agent Advertisement (care-of-address)
Registration Request(care-of-address)
Registration Request
Foreign Directory Server
Dir-Access-Request
Dir-Access-Response
Radius Access Request (Registration Request)
Home Directory Server
Dir-Access-Request
Dir-Access-Response
Home IWF & PPP Server
Home Acctg Server
Start-IWF-Request
Radius-Accig-Start-Request
Radius-Accig-Start-Response
Start-IWF-Response
Radius Access Response (Registration Reply)
Serving IWF
Serving Acctg Server
Start-IWF-Request
Radius-Accig-Start-Request
Radius-Accig-Start-Response
Start-IWF-Response
Registration Reply
Registration Reply
Agent Discovery Phase
Registration Phase
LCP Config Request
LCP Config Request
LCP Configure-Ack
LCP Configure-Ack
PAP Authenticate-Request
PAP Authenticate-Request
PAP Authenticate-Ack
PAP Authenticate-Ack
IPCP Configure-Request
IPCP Configure-Request
IPCP Configure-Ack
IPCP Configure-Ack
PPP Link Establishment Phase
PPP Authentication Phase
PPP Network Config Phase

FIG. 14

FIG. 15

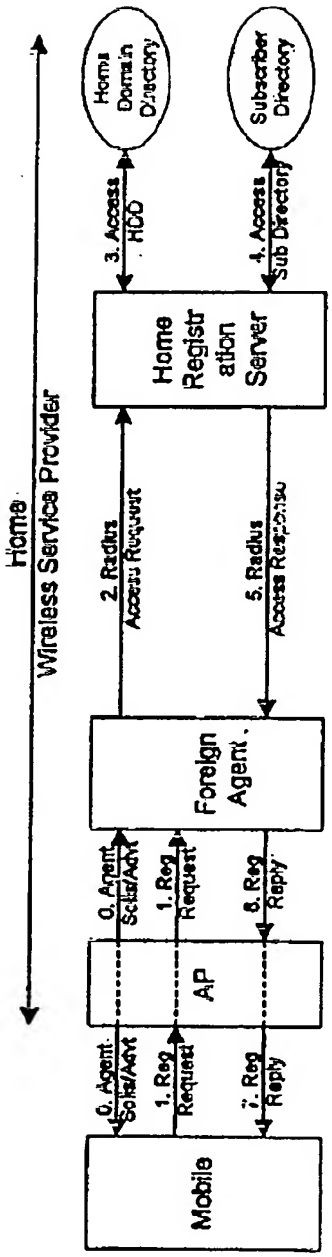

Home Wireless Service Provider
Home Domain Directory
Subscriber Directory
3. Access HDD
4. Access Sub Directory
Home Registration Server
2. Radius Access Request
5. Radius Access Response
Foreign Agent
0. Agent Solicit/Advt
1. Reg Request
6. Reg Reply
AP
0. Agent Solicit/Advt
1. Reg Request
6. Reg Reply
Mobile

FIG. 16

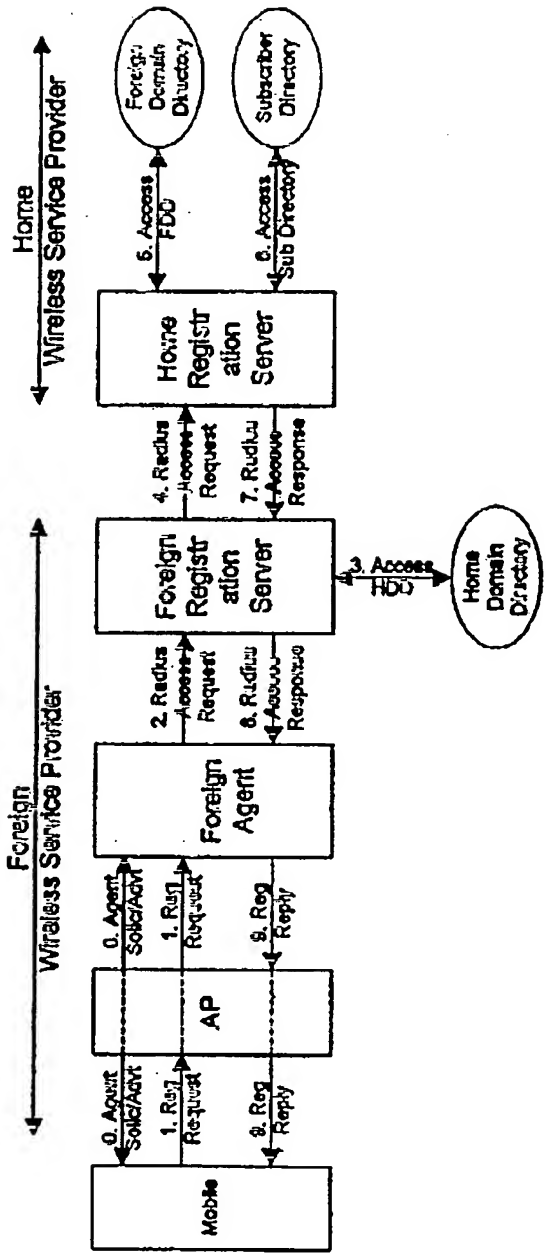

Home
Wireless Service Provider
Foreign
Wireless Service Provider
Foreign Domain Directory
Subscriber Directory
Home Registration Server
Foreign Registration Server
Home Domain Directory
Foreign Agent
AP
Mobile
5. Access FDD
6. Access Sub Directory
4. Radius Access Request
7. Radius Access Response
3. Access HDD
2. Radius Access Request
8. Radius Access Response
0. Agent Solicit/Advt
1. Reg Request
9. Reg Reply
0. Agent Solicit/Advt
1. Reg Request
9. Reg Reply

FIG. 17

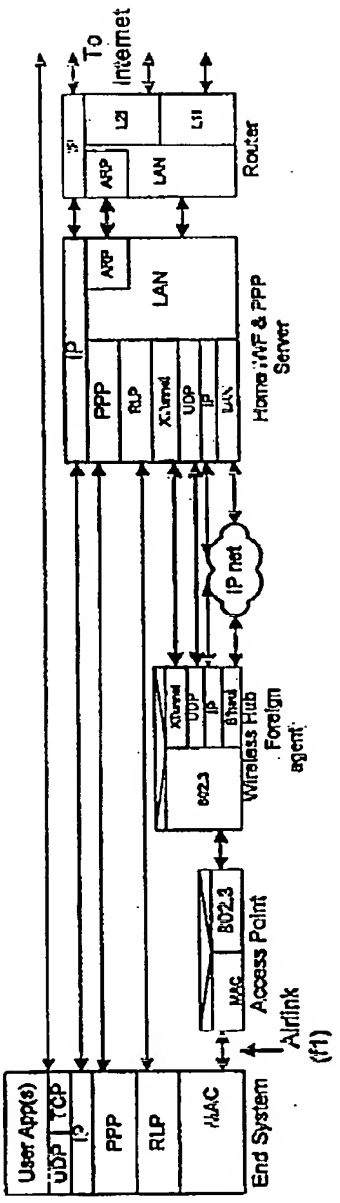

To Internet
L2
L1
ARP
LAN
Router
IP
ARP
LAN
PPP
RLP
Xchnnl
UDP
IP
LAN
Home IWF & PPP Server
IP net
Xchnnl
UDP
IP
Ethnnl
802.3
Wireless Hub
Foreign agent
802.3
MAC
Access Point
Airlink
(f1)
User App(s)
TCP
UDP
IP
PPP
RLP
MAC
End System

FIG. 18

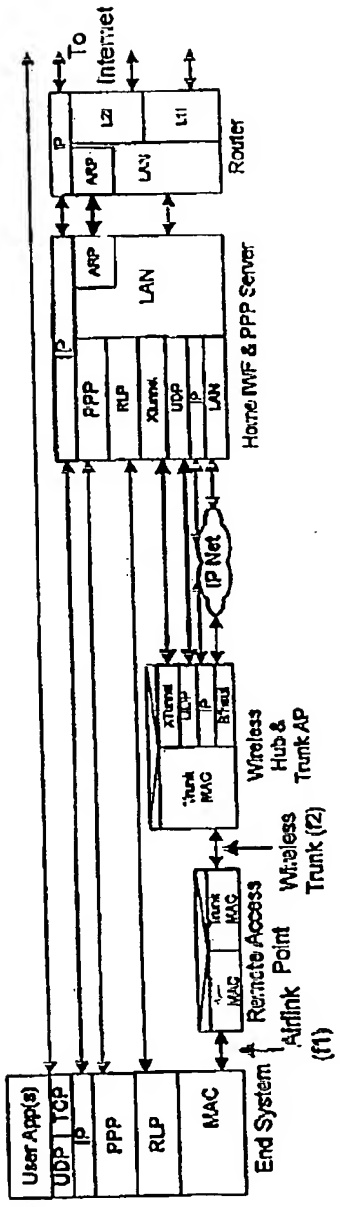

To Internet
L2
L1
ARP
LAN
Router
IP
ARP
LAN
PPP
RLP
Xchnnl
UDP
IP
LAN
Home IWF & PPP Server
IP Net
Xchnnl
UDP
IP
Ethnnl
Trunk MAC
Wireless Hub & Trunk AP
Trunk MAC
MAC
Remote Access Point
Wireless Trunk (f2)
Airlink
(f1)
User App(s)
TCP
UDP
IP
PPP
RLP
MAC
End System

FIG. 19

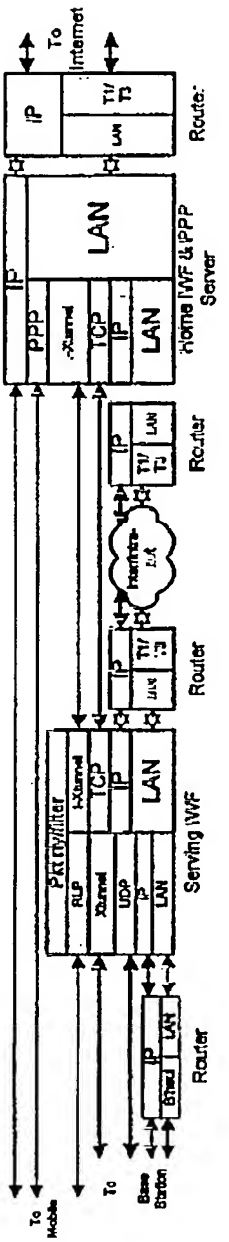

To Internet
IP
TV/T3
LAN
Router
LAN
IP
PPP
X.tunnel
TCP
IP
LAN
Home IWF & PPP Server
IP
TV/T3
LAN
Router
Internet
IP
TV/T3
LAN
Router
PktFilter
RUP
X.tunnel
TCP
IP
LAN
X.tunnel
UDP
IP
LAN
Serving IWF
IP
Ethernet
LAN
Router
To Mobile
To Base Station

FIG. 20

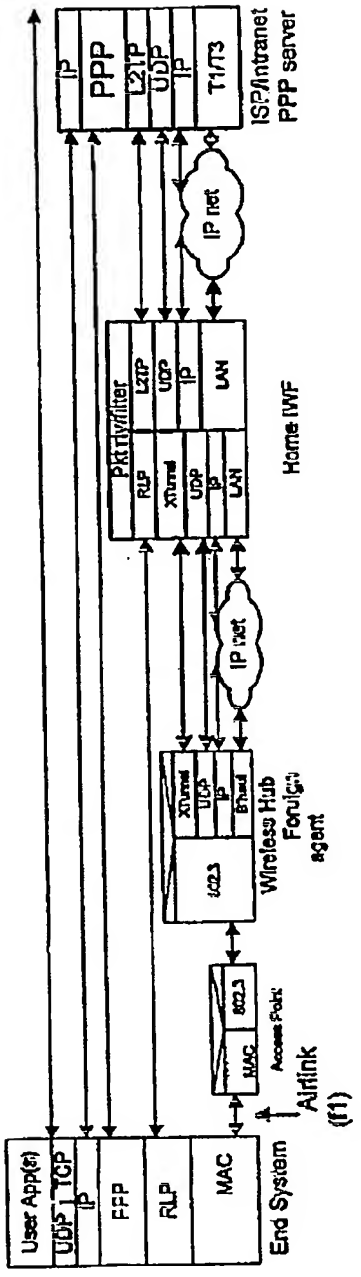

User App(s)
UDP
TCP
IP
PPP
RLP
MAC
End System
Airlink
(f1)
Access Point
802.3
MAC
Wireless Hub
Foreign agent
Home IWF
PktTrnfrAfter
RLP
XTunnel
UDP
IP
LAN
IP net
ISP/Intranet
PPP server
T1/73
L2TP

FIG. 21

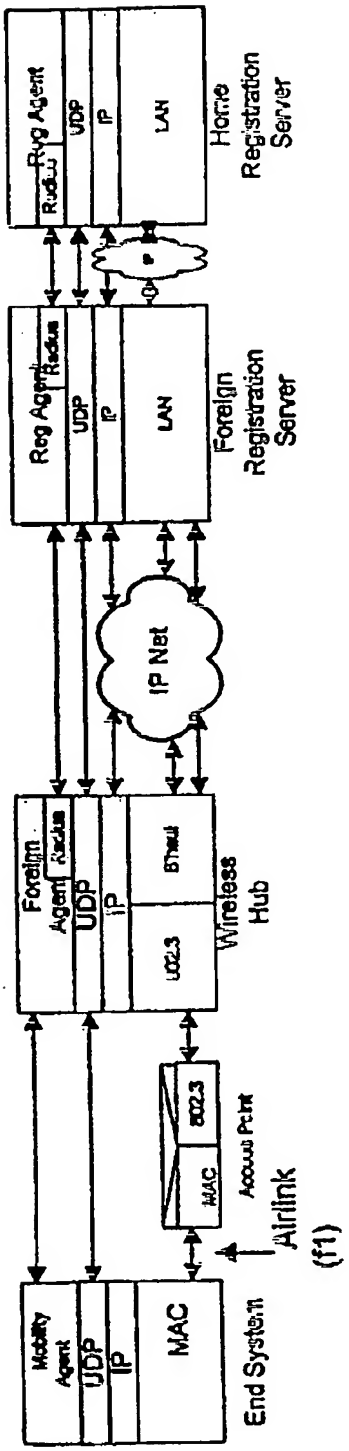

Mobility Agent
UDP
IP
MAC
End System
Airlink
(f1)
Access Point
802.3
MAC
Wireless Hub
Foreign Agent
Radius
UDP
IP
Btwd
802.3
IP Net
Reg Agent
Foreign Registration Server
Home Registration Server
LAN

FIG. 22

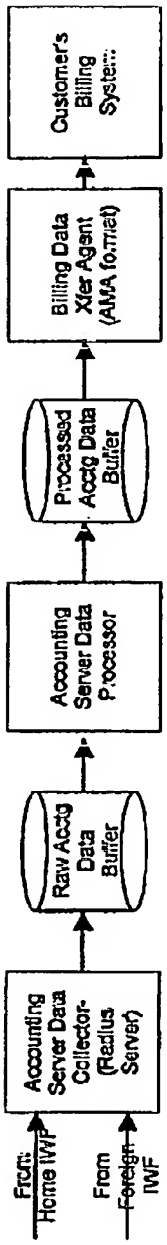

From Home IWF
From Foreign IWF
Accounting Server Data Collector- (Radius Server)
Raw Acctg Data Buffer
Accounting Server Data Processor
Processed Acctg Data Buffer
Billing Data Xfer Agent (AMA format)
Customer's Billing System

FIG. 23

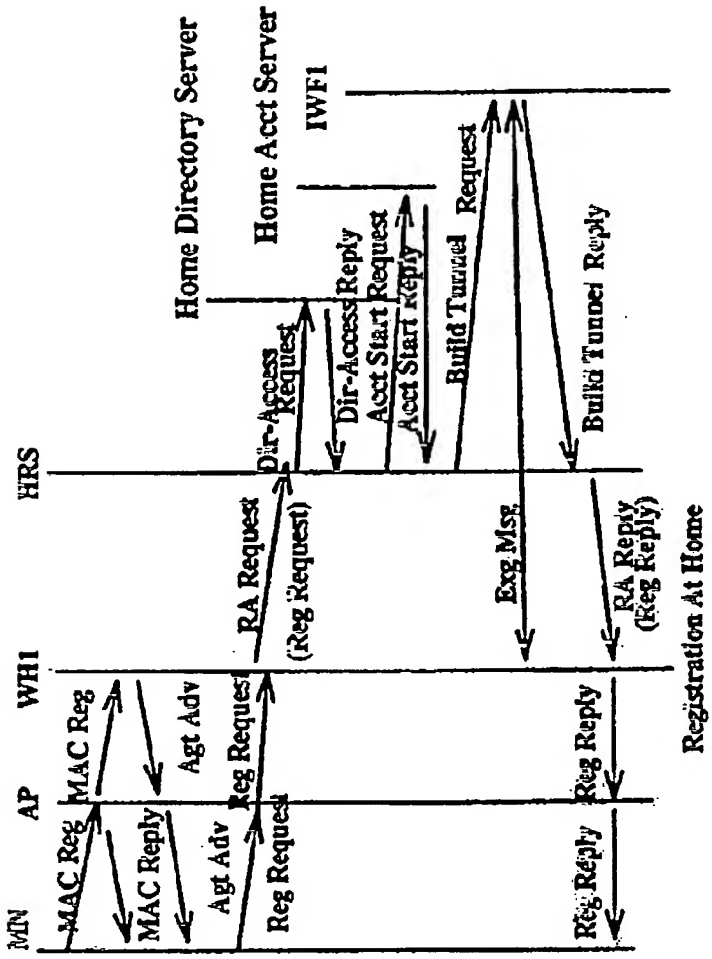

MN
AP
WH1
HRS
IWF1
Home Acct Server
Home Directory Server
MAC Reg
MAC Reply
Agt Adv
Reg Request
RA Request
(Reg Request)
Dir-Access Request
Dir-Access Reply
Acct Start Request
Acct Start Reply
Build Tunnel Request
Build Tunnel Reply
Exg Msg
RA Reply
(Reg Reply)
Reg Reply
Registration At Home

FIG. 24

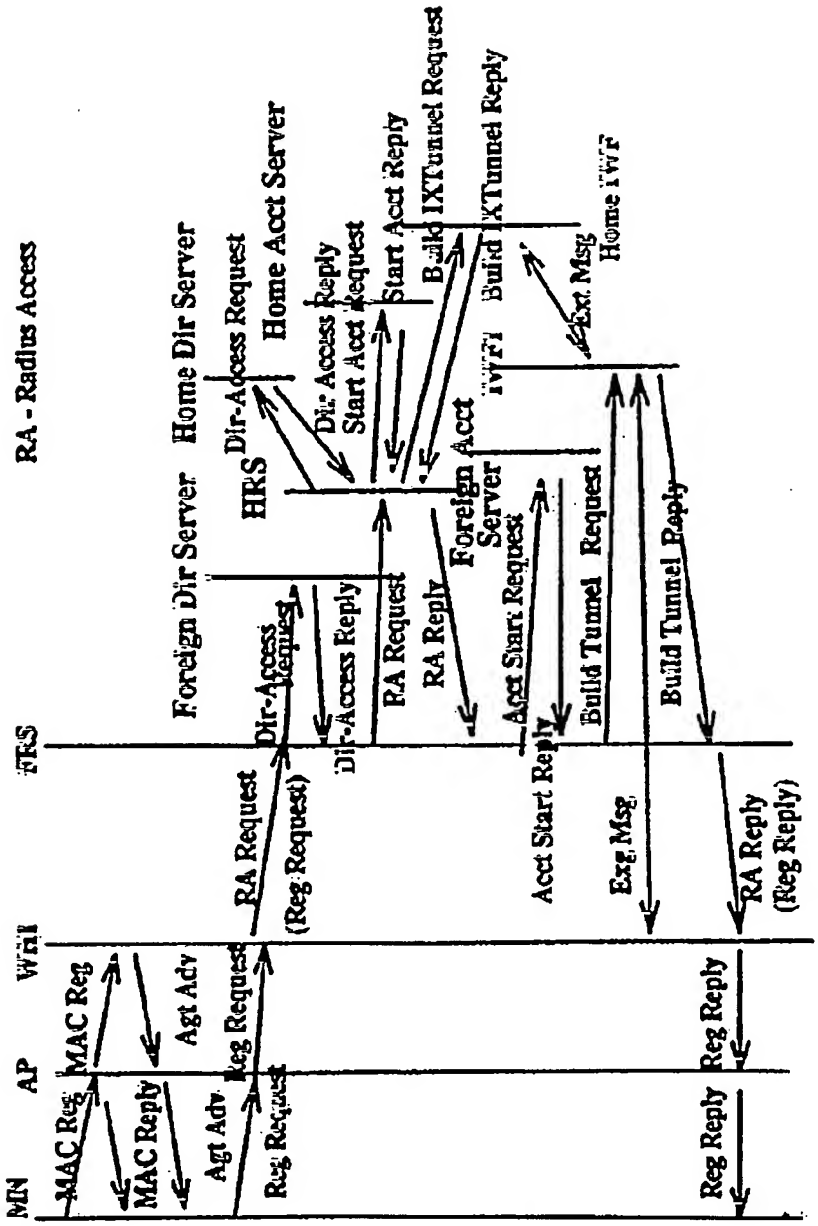

MN
AP
WRI
FRS
RA - Radius Access
Foreign Dir Server
Home Dir Server
HRS
Home Acct Server
Foreign Acct Server
Home IWF
MAC Reg
MAC Reply
Agt Adv
Reg Request
RA Request (Reg Request)
Dir-Access Request
Dir-Access Reply
RA Request
RA Reply
Acct Start Request
Acct Start Reply
Build Tunnel Request
Build Tunnel Reply
Exg Msg
Reg Reply
RA Reply (Reg Reply)
Dir-Access Request
Dir-Access Reply
Start Acct Request
Start Acct Reply
Build IXTunnel Request
Build IXTunnel Reply
Exg Msg

FIG. 25

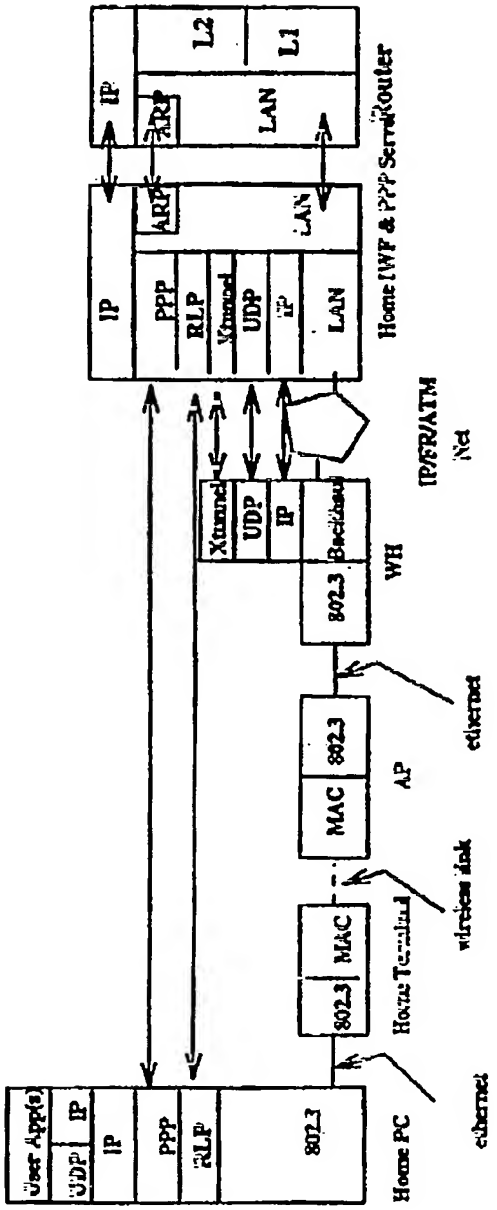

L2
L1
IP
ARP
LAN
Home IWF & PPP Server/Router
PPP
RLP
Xtunnel
UDP
IP
LAN
IP/FR/ATM
Net
802.3
WH
MAC
AP
ethernet
wireless link
Home Terminal
Home PC
User App(s)
TCP

FIG. 26

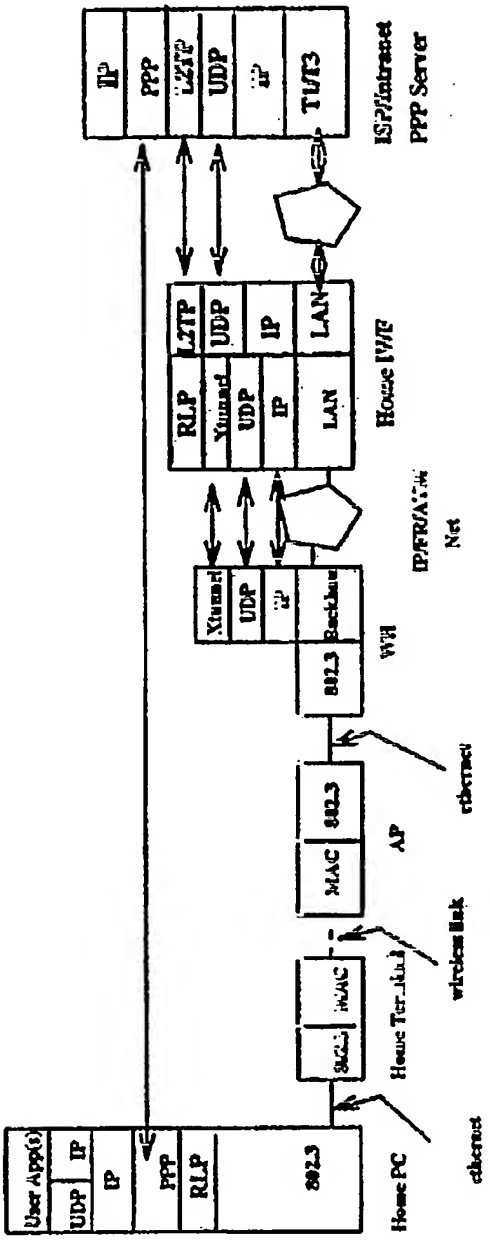
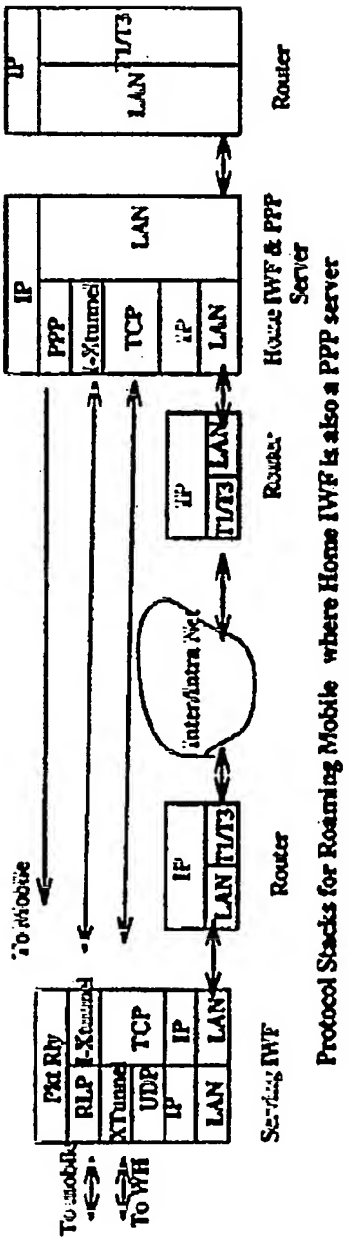
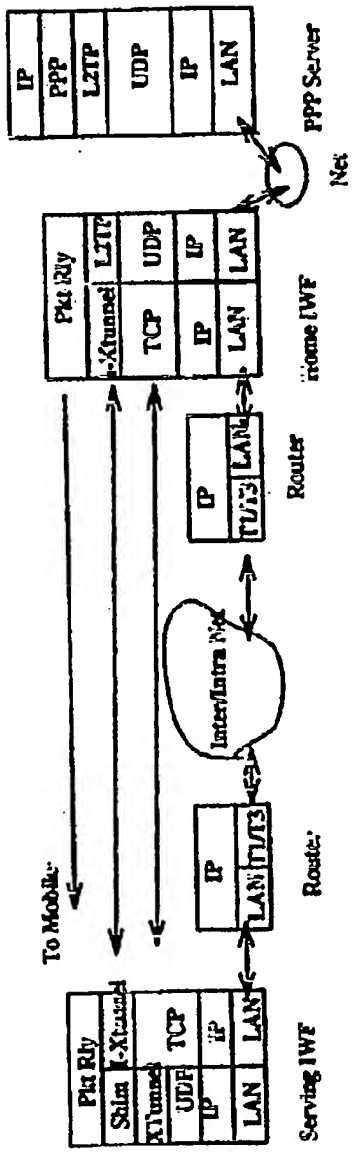

IP
PPP
UDP
T1/E3
ISP/Intranet
PPP Server
LAN
House PNF
RLP
UDP
IP
Net
802.3
AP
MAC
ethernet
wireless link
Home PC
User App(s)
RLP

FIG. 27



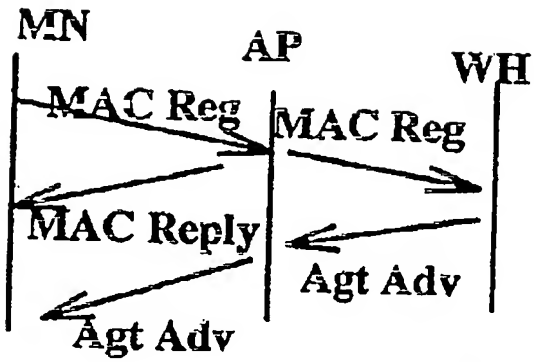
Protocol Stacks for Roaming Mobile where Home IWF is also a PPP server

FIG. 28



Protocol Stacks for Roaming Mobile when Home IWF and PPP Server are separate

FIG. 29



Local Handoff

FIG. 30

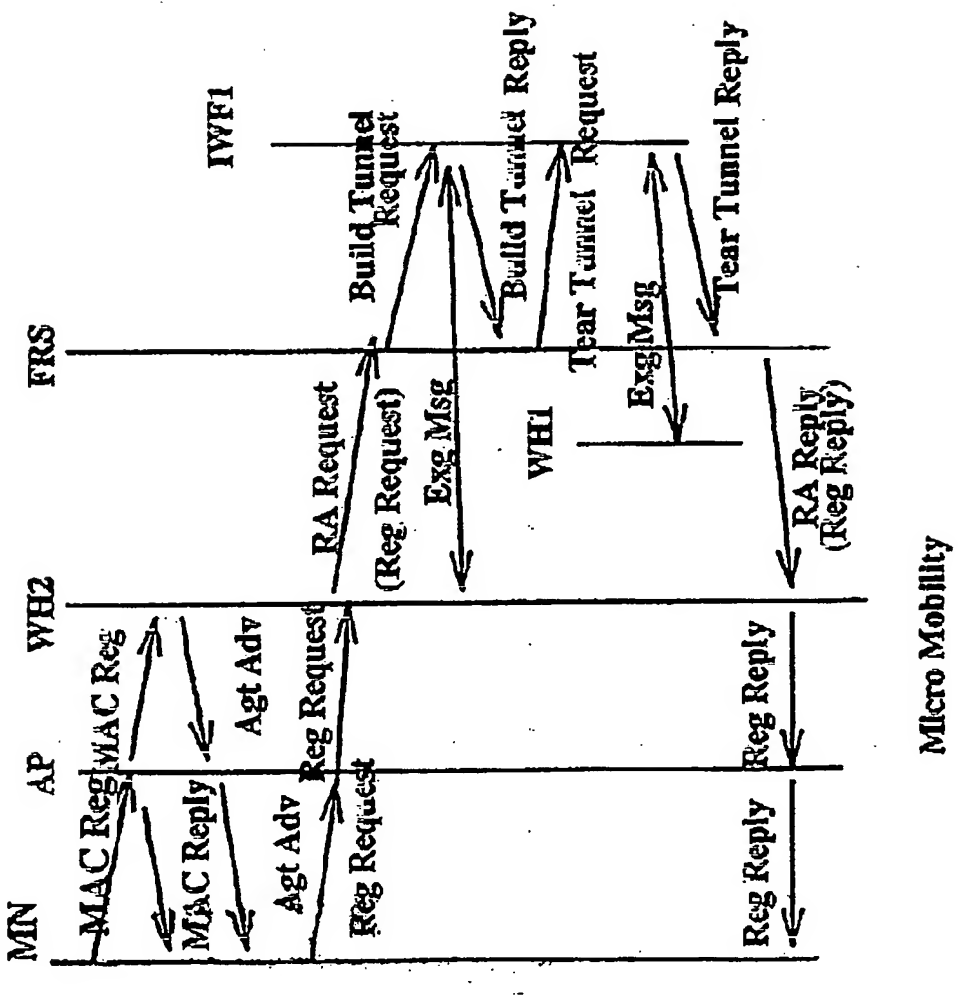

MN
AP
WH2
FRS
IWF1
WH1
MAC Reg
MAC Reply
Agt Adv
Reg Request
RA Request
(Reg Request)
Exg Msg
Build Tunnel Request
Build Tunnel Reply
Tear Tunnel Request
Exg Msg
Tear Tunnel Reply
RA Reply
(Reg Reply)
Reg Reply
Reg Reply
Micro Mobility

FIG. 31

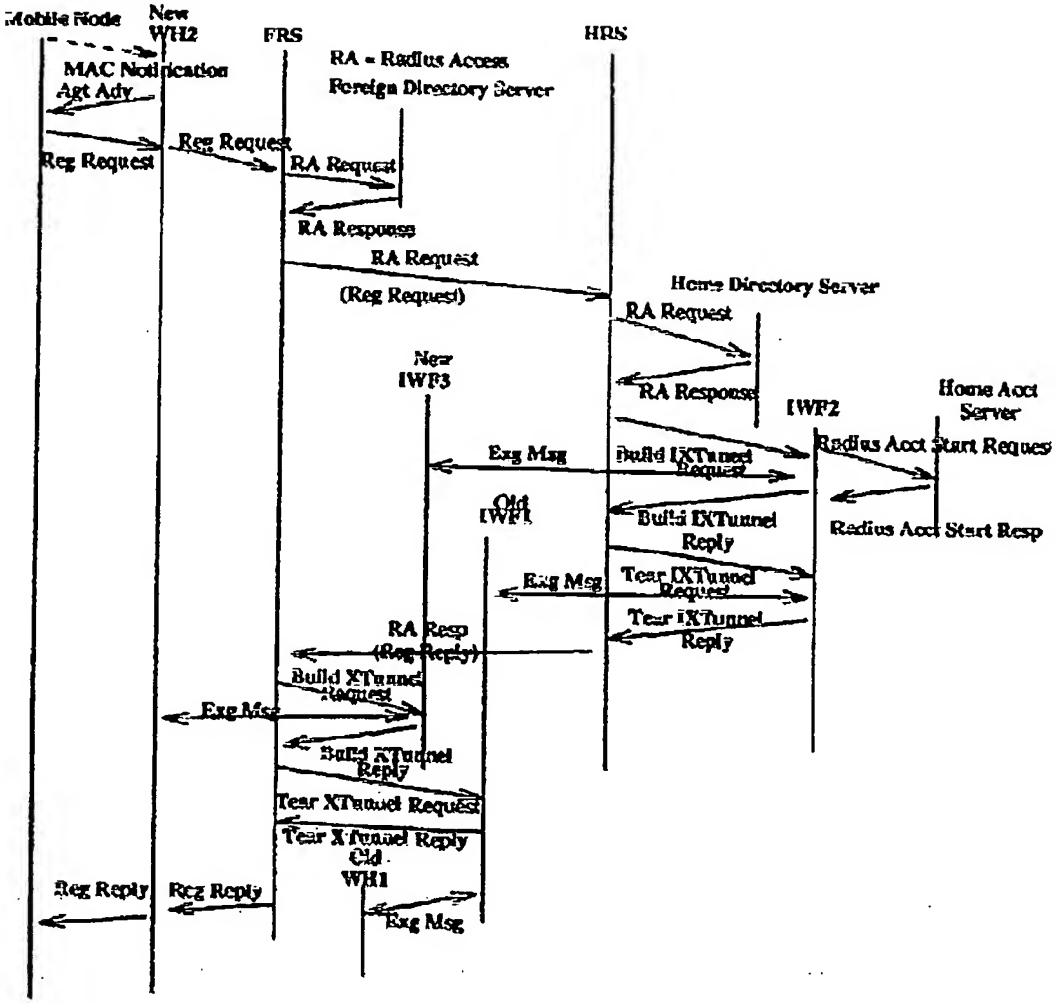

Mobile Node
New WH2
FRS
HRS
RA = Radius Access
Foreign Directory Server
MAC Notification
Agt Adv
Reg Request
Reg Request
RA Request
RA Response
RA Request
(Reg Request)
Home Directory Server
RA Request
RA Response
New IWF3
IWF2
Home Acct Server
Exg Msg
Build IXTunnel Request
Radius Acct Start Request
Old IWF1
Build IXTunnel Reply
Radius Acct Start Resp
Exg Msg
Tear IXTunnel Request
Tear IXTunnel Reply
RA Resp
(Reg Reply)
Build XTunnel Request
Exg Msg
Build XTunnel Reply
Tear XTunnel Request
Tear XTunnel Reply
Old WH1
Reg Reply
Reg Reply
Exg Msg

FIG. 32

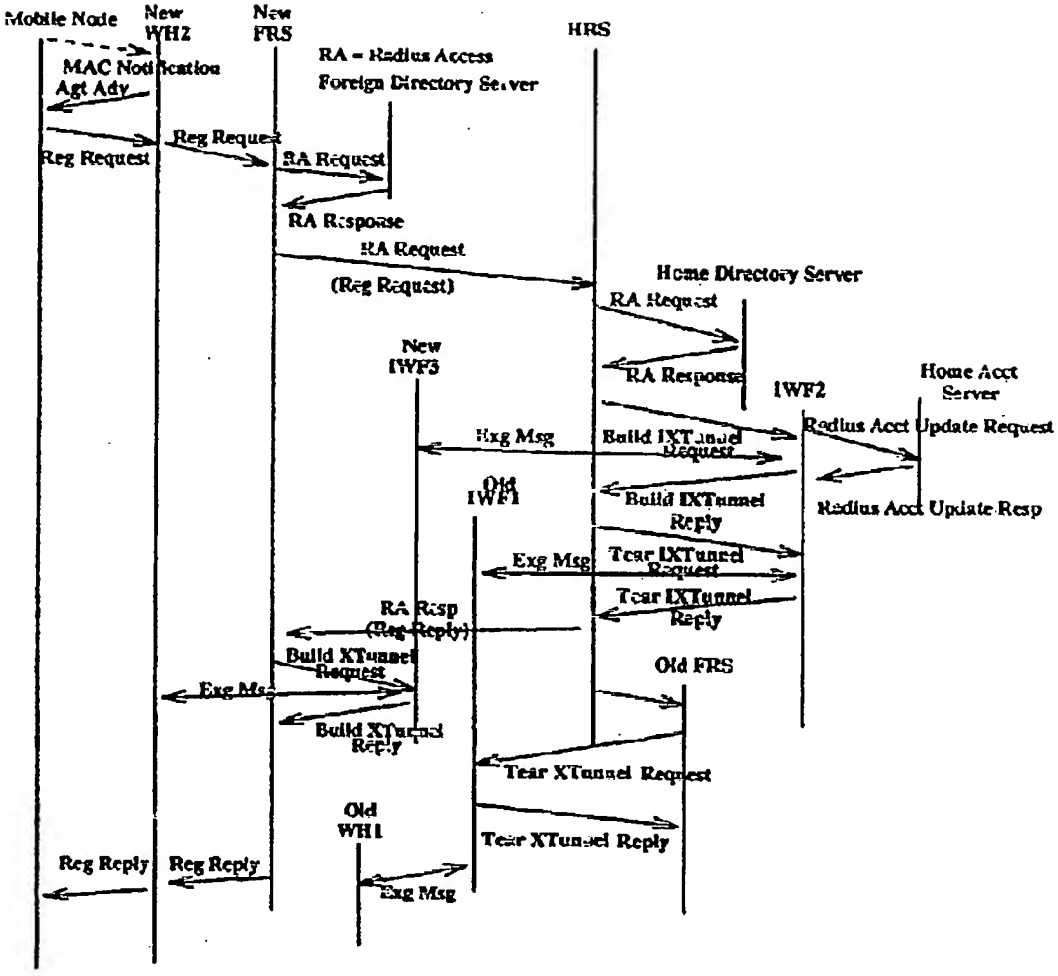

Mobile Node
New WH2
New FRS
HRS
RA = Radius Access
Foreign Directory Server
MAC Notification
Agt Adv
Reg Request
Reg Request
RA Request
RA Response
RA Request
(Reg Request)
Home Directory Server
RA Request
RA Response
New IWF3
IWF2
Home Acct Server
Exg Msg
Build IXTunnel Request
Radius Acct Update Request
Old IWF1
Build IXTunnel Reply
Radius Acct Update Resp
Exg Msg
Tear IXTunnel Request
Tear IXTunnel Reply
RA Resp
(Reg Reply)
Build XTunnel Request
Old FRS
Exg Msg
Build XTunnel Reply
Tear XTunnel Request
Old WH1
Tear XTunnel Reply
Reg Reply
Reg Reply
Exg Msg

FIG. 33

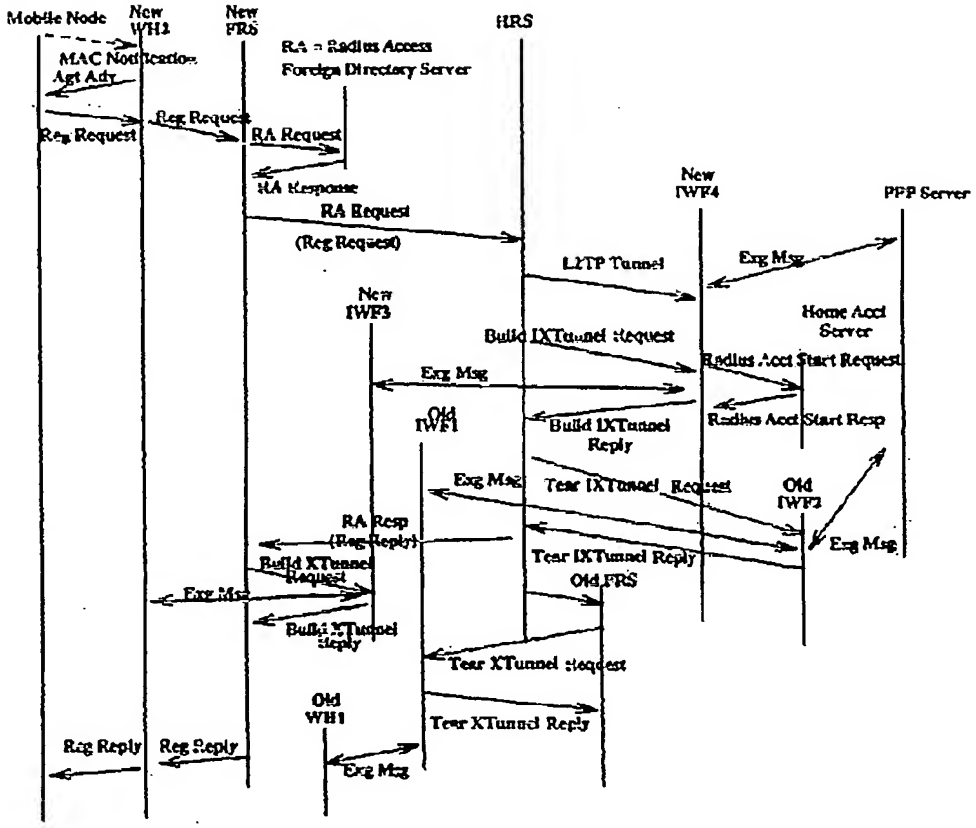
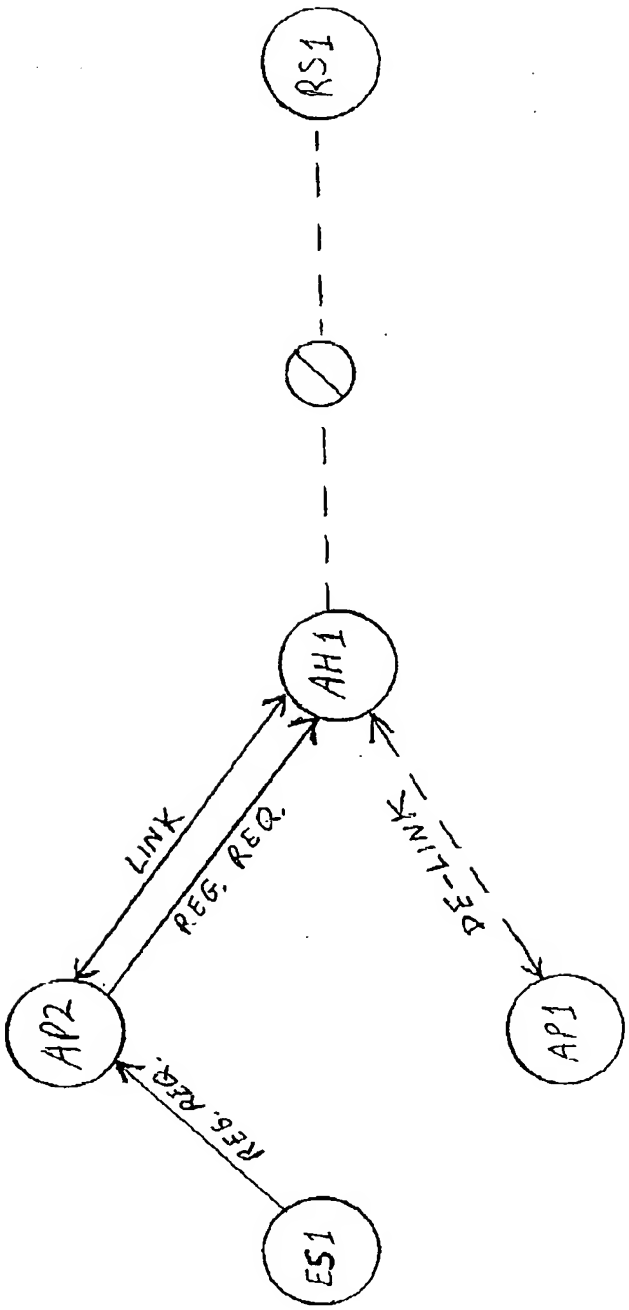

Mobile Node
New WH1
New FR5
HRS
RA = Radius Access
Foreign Directory Server
MAC Notification
Agt Adv
Reg Request
Reg Request
RA Request
RA Response
RA Request
(Reg Request)
New IWF4
PPP Server
L2TP Tunnel
Exg Msg
New IWF3
Home Acct Server
Build IXTunnel Request
Radius Acct Start Request
Exg Msg
Old IWF1
Build IXTunnel Reply
Radius Acct Start Resp
Exg Msg
Tear IXTunnel Request
Old IWF2
RA Resp
(Reg Reply)
Exg Msg
Tear IXTunnel Reply
Build XTunnel Request
Old FR5
Exg Msg
Build XTunnel Reply
Tear XTunnel Request
Old WH1
Tear XTunnel Reply
Reg Reply
Reg Reply
Exg Msg

FIG. 34



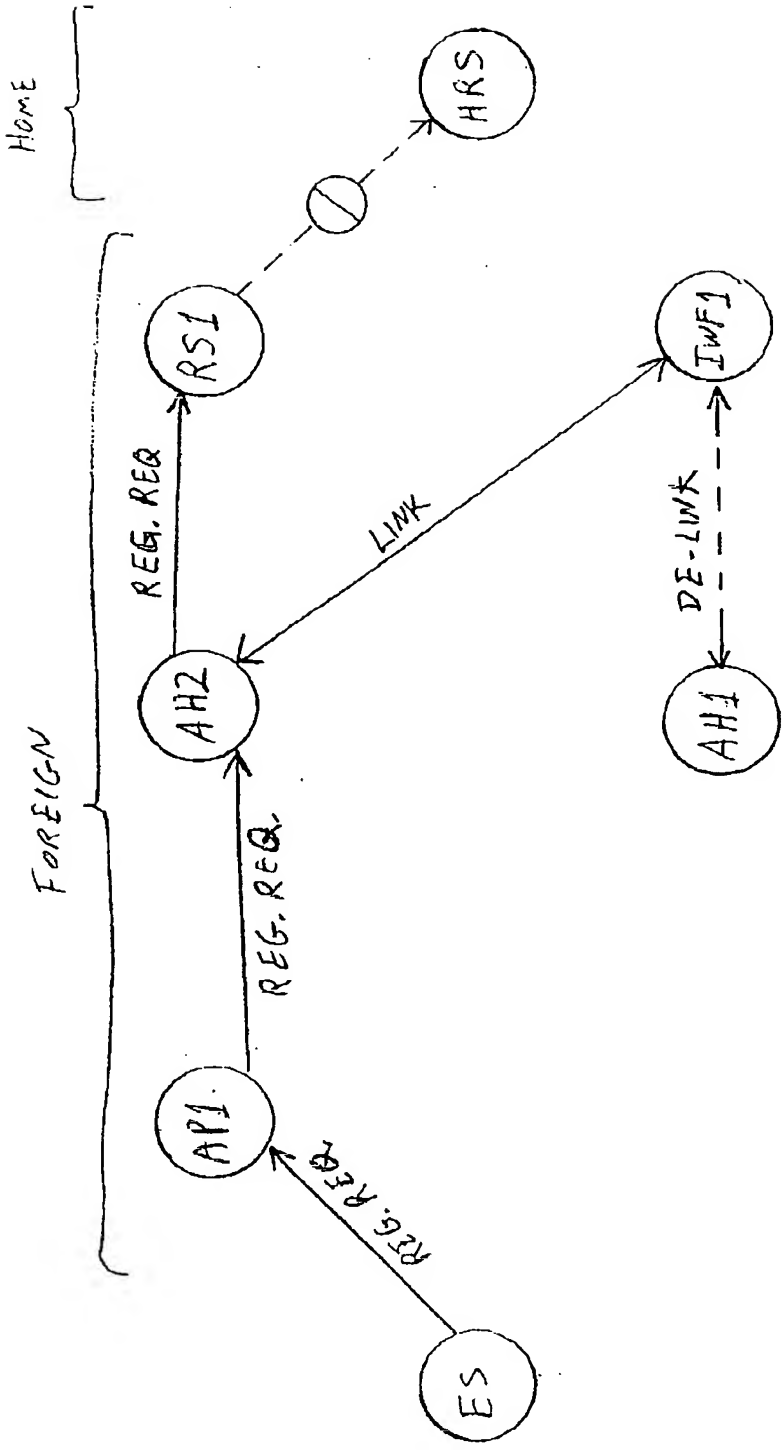

HOME
HRS
RS1
IWF1
REG. REQ
LINK
DE-LINK
AH2
AH1
FOREIGN
REG. REQ.
AP1
REG. REQ.
ES

FIG. 35

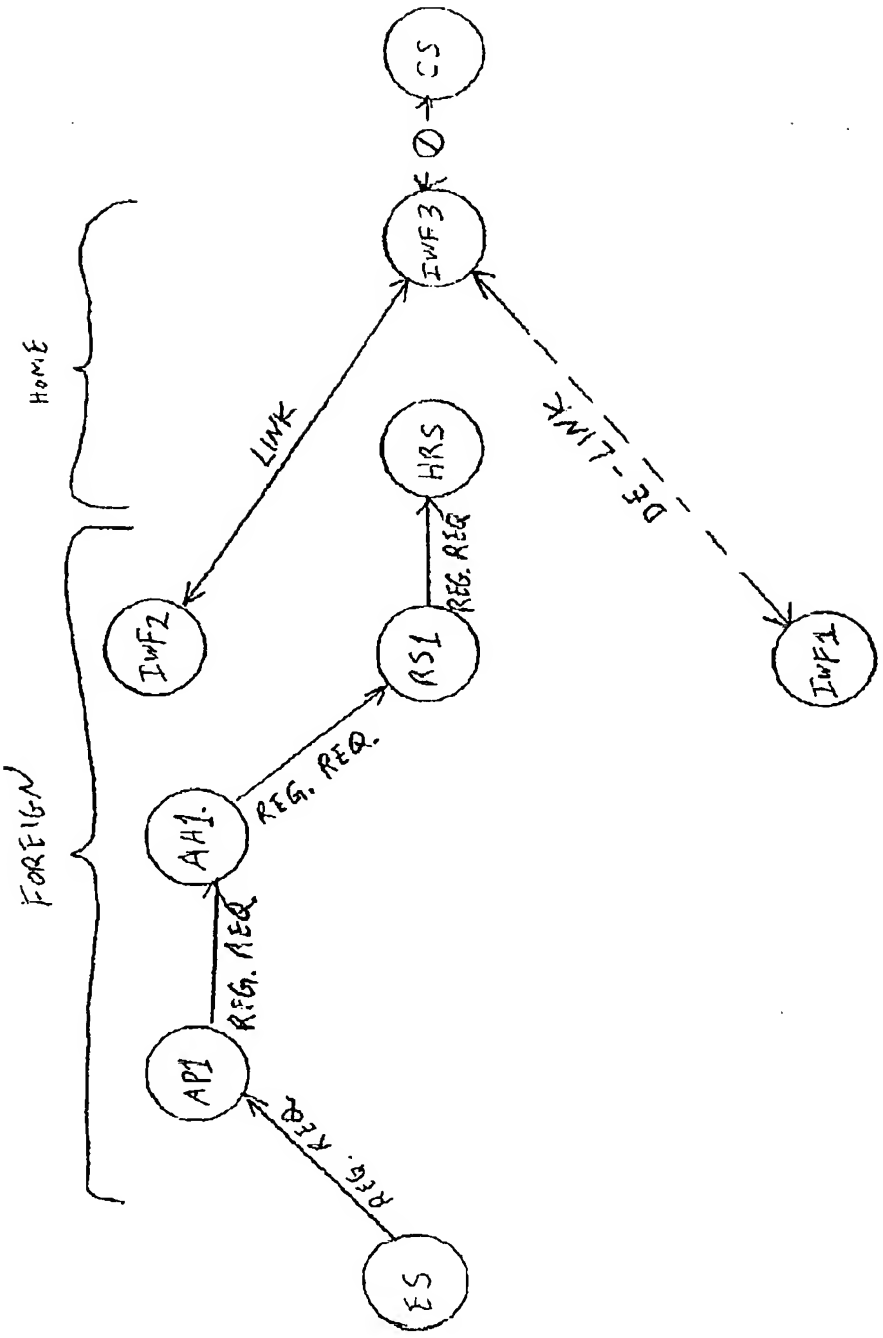

CS
IWF3
HOME
LINK
HRS
DE-LINK
REG. REQ
IWF2
RS1
IWF1
REG. REQ.
AH1.
REG. REQ
AD1
REG. REQ
ES
FOREIGN

FIG. 36

FIG. 37

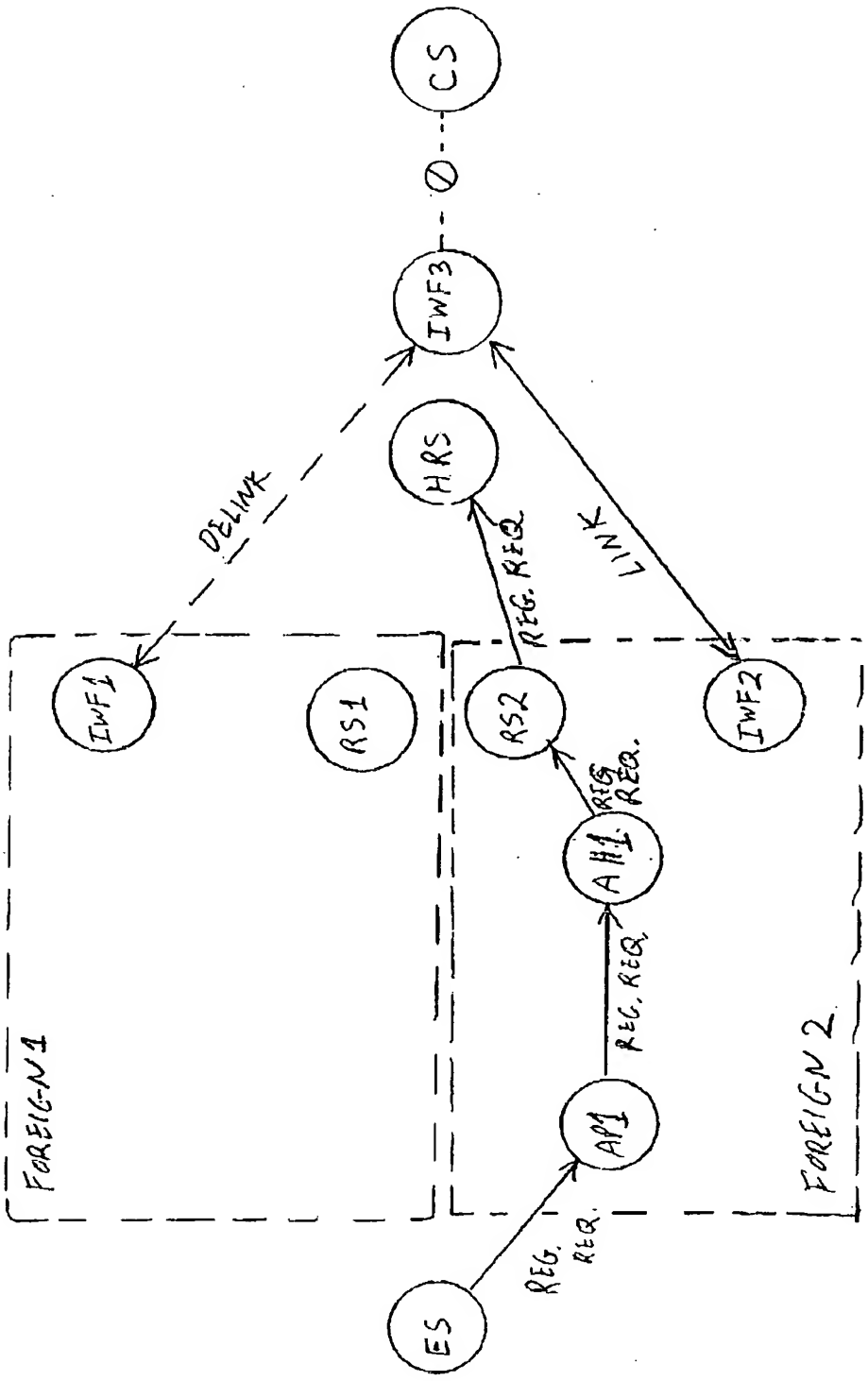
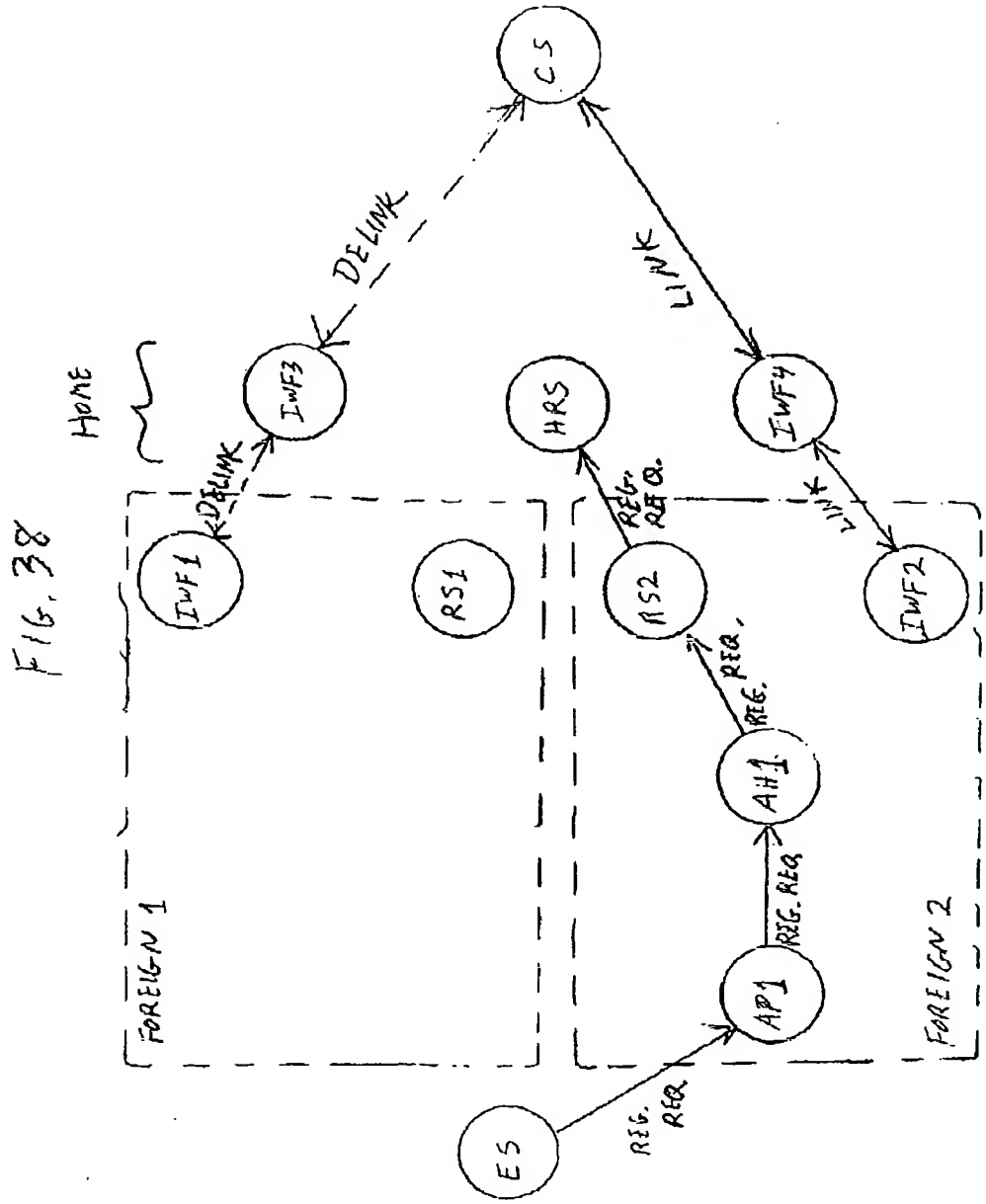

CS
IWF3
H.RS
DELINK
LINK
REG. REQ.
IWF1
RS1
RS2
IWF2
REG. REQ.
AH1
REG. REQ.
REG. REQ.
AP1
REG. REQ.
ES
FOREIGN 1
FOREIGN 2

FIG. 38


CS
DELINK
LINK
HOME
IWF3
HRS
IWF4
REDELINK
REG. REQ.
IWF1
RS1
RS2
IWF2
LINK
REG. REQ.
AH1
REG. REQ
AP1
FOREIGN 1
FOREIGN 2
ES
REG. REQ

1. Abstract

A wireless data network includes a wireless packet switched data network for end users that divides mobility management into local, micro, macro and global connection handover categories and minimizes handoff updates according to the handover category. The network integrates MAC handoff messages with network handoff messages. The network separately directs registration functions to a registration server and direct routing functions to inter-working function units. The network provides an intermediate XTunnel channel between a wireless hub (also called access hub AH) and an inter-working function unit (IWF unit) in a foreign network, and it provides an IXTunnel channel between an inter-working function unit in a foreign network and an inter-working function unit in a home network. The network enhances the layer two tunneling protocol (L2TP) to support a mobile end system, and it performs network layer registration before the start of a PPP communication session.

2. Representative Drawing

FIG. 2